JASA-22-01

平成22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23年3月　社団法人　組込みシステム技術協会

JASA-22-01

平成22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23年3月

社団法人　組込みシステム技術協会

KEIRIN

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

セキュリティワーキンググループ

はじめに

本セキュリティワーキンググループ（WG）は今までISO/IEC 15408、情報セキュリティの組織管理などを調査研究してまいりました。本年度は組込みシステムの技術的側面に焦点を当てました。

折しもIPA（情報処理推進機構）様が、『組込みシステムのセキュリティへの取組みガイド（2010年度改訂版）』を出されるなど、組込みシステムへの取組みを強化しております。このようなことから、本セキュリティWGでは、IPA様と連携を取らせていただき、組込み業界が抱えているセキュリティの課題に関して、研究の協力をいただきました。外部との連携が本年度の大きな特徴になっており、いままでの研究成果の1つと考えております。

本調査報告は以下、主に４つの内容を収録しております。１つは『ガイド』をもとにセキュリティの技術の調査を行いました。本WGの調査によれば、情報セキュリティに関するハードウェアの側面からの知識情報が少ないと考えられます。そこで、『ガイド』に使用されている用語の調査を行いました。本内容からセキュリティに関するハードウェアの知見が獲得されると思われます。IPA様より協力を得ております。

２つ目は、協会企業様が、組込みシステムの開発ライフサイクルに応じたセキュリティ対策をどう講じられているか、アンケート調査を行いました。その結果を掲載しております。アンケート項目の設定はIPA様の協力を得ております。以前は組織全般の情報セキュリティ管理の状況をアンケート調査させていただきましたが、今回は技術的側面に応じた調査となっております。またこのアンケートは本協会らしく、ネット技術を活用したものとさせていただきました。

３つ目は、本WGのメンバーによる、Linux、仮想化、クラウドの３つの観点から情報セキュリティに関する最近の議論を展開させていただいております。情報セキュリティの課題は新たなプラットフォームが誕生すれば、必ずついてまわり、議論を整理しておく必要のある課題です。

４つ目は、IPA様からは『ガイド』全般にまつわるご講演、また車載システムの情報セキュリティに関する、米国での研究などをご講演いただきました。この講演内容も本報告書に収めております。

なおこのアンケートはこれまでの研究成果を踏まえて、コンパクトで的を射た、経済的な負担の少ない情報セキュリティ管理制度を協会として作るための、基礎資料とさせていただく予定です。本制度も来年度を目指して、セキュリティWGにて検討しております。

会員各位におかれましては、本報告書をご活用いただきたく存じます。

最後に本事業を支援いただきました財団法人ＪＫＡ様に感謝申し上げます。

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

目次（第1部）

第1章
ハードウェア関連キーワードに関する調査報告

本章は、独立行政法人情報処理推進機構（IPA）が発行する「組込みシステムのセキュリティへの取組みガイド（2010年度改訂版）」（以下、ガイド）に基づいて、組込みシステムのセキュリティを理解するのに必要な基礎知識について解説する。

JASAは2010年10月にETセミナー「自動車等組込みシステムのセキュリティ技術」を開催し、IPAより講師3氏を招いて組込みシステムのセキュリティの現状、研究成果、脅威について講演いただいた。

本報告は、IPAと提携したセキュリティ推進活動の一環として当ワーキンググループが行った調査結果を、項目ごとにまとめたものである。ガイドから組込み技術者教育で留意すべきと思われる用語（**表1.1**）を抽出し、これらについて調査を行った。ガイドでは、ハードウェアに関する言及がソフトウェアに関するものに比較して少ないように思われたことから、今年度は表中の用語から、特にハードウェア関連用語について優先的に調査を行い、その結果を報告する。なお、各項目名の後のページ数はガイドに記載されたページ数を表す。

表1.1　ガイドで取り上げられた用語の一部

TPM（Trusted Platform Module）	情報家電 ・ 家庭内制御系	BGA
開発用のデバッグコネクタ（JTAG）	サービスマン用の通信端子	故障利用攻撃
バス暗号化（Bus encryption）	リバースエンジニアリング攻撃	ベンダーコード
（記憶装置の）物理的消去機能		

1.1　TPMについて　(p.5)

「Trusted Platform Module」の略で、データの暗号化や復号、鍵情報を安全に格納する機能を持ったセキュリティICチップ。主要ITベンダからなる業界団体のTCG(Trusted Computing Group)により仕様が策定されている。

TCGは、セキュアなコンピュータプラットフォームを構築するための、ハードウェア、ソフトウェアの業界標準仕様の開発、普及することを目的とした業界団体(非営利組織)で、特定ベンダに依存しない、信頼できるコンピューティング・プラットフォームを実現する業界標準仕様の開発とその普及の促進を目的としている。その活動の1つとして、TPMを信頼の要とする信頼できるアプリケーションの実行環境を構築するためのTPMセキュリティチップを提案している。TPMは、パソコンなどのマザーボード上に取り付けられ、信頼できるコンピュータを実現するための、端末側の信頼基点となる。ここで、TCGにおける信頼とは、「プラットフォームに想定外の改変が加えられないこと、即ち「システムが意図した通りに動作すること」の保証を意味している。**図1.1**に示すように、ソフトウェアからの不正ができないような耐タンパ領域（＝セキュアチップ）をプラットフォームに埋め込み、これを信頼のルート（Root of Trust）として、改ざんが極めて困難な、信頼できるコンピューティング環境を構築している。

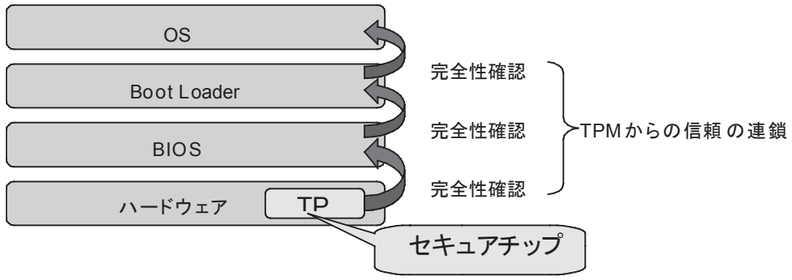


図1.1　セキュアなコンピュータプラットフォーム

（参考 ： Business Communication@net最新技術トレンド
http://www.bcm.co.jp/site/2004/2004Feb/techo-trend/04techo-trend02.htm）

TPMは次のような考え方により、通常ソフトウェアで実行されている処理よりも高いセキュリティレベルを、ハードウェアで実現している。

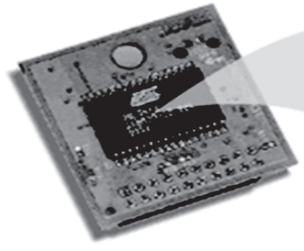
(1) 信頼できるプラットフォームの実現 ： 上記のように、TPMを起点としてBIOS、ブートレコード、OSに至るソフトウェアの完全性を検証するため、ハッシュ値を計算・保存することによって、安全なアプリケーションの実行環境を実現する。

(2) ハードウェアベースのデータ・証明書の保護 ： ハードウェアの堅牢性に基づいたデータの保護環境を提供することによって、情報漏洩リスクを低減する。

(3) 安全な暗号処理環境の実現 ： 暗号鍵の生成・利用・破棄に至る全ライフサイクルにわたって堅牢なTPM内で管理することによって、安全な暗号処理や電子署名を可能とする。

(4) TCO（Total Cost of Ownership）の削減 ： 実装される機能、メモリ保護領域、プロセッサ・パワーを極力抑えて設計されており、低コストでの製造、さらにデバイス機器やプラットフォームへの適用を可能とする。

TPMの基本的な機能としては、**図1.2**のようになる。



	乱数生成装置		不揮発性メモリ
I/O	プロセッサー		メモリ
	SHA-1	非対称暗号鍵生成	署名と暗号
	RSA		
	時計/タイマー		電源検出

写真はIBM＞Lenovo「セキュリティ・チップ(TPM)」参照
http://www-06.ibm.com/jp/pc/think/security/chip.shtml

TPMの基本機能

・プラットフォームの正当性検証 ： PCの起動時に、TPMはTCGの仕様に定められた方法でプラットフォームとの認証を取り行う。プラットフォームに不正な改ざんがあった場合や別のTPMと取り替えた場合、またはTPMを取り外した場合などは、認証エラーとなり起動することができなくなる。

・インテグリティの観測 ： TPMでコンポーネント(ハードウェアやソフトウェア)が正当なものをハッシュを使用して測定する。 予め定められた値の正さを積み重ねていくことで、ハードウェア→BIOS→Boot Loader→OS→アプリケーションの順に「信頼の連鎖」を作ることによって、ハードやソフトが改ざんされていないかをチェックする。

・RSA（公開暗号方式の1つ）暗号の秘密鍵の生成・保管・演算（暗号化・復号・署名）

・SHA-1（Secure Hash Algorithm-1:認証やデジタル署名などに使われるハッシュ関数の１つ）によるハッシュ演算

・暗号鍵の保護 ： TPMには暗号鍵を入れる保護するための場所として、EEPROM(書込み可能な不揮発性メモリ)を有する。通常、TPMの鍵がコアの鍵となり、アプリケーションの暗号鍵を暗号化することによって安全に使用できる。 TPM内に保存された暗号鍵は通常の方法では、他のPCなど外に出せない。

・暗号処理機能 ： TPM内で次の処理を行う。乱数生成機能、RSA暗号処理(2048bit)、ハッシュ関数。

・その他 ： I/Oや時計/タイマー、電源検出

図1.2　TPMの基本機能構成

2003年11月にTCGからTPM1.2が発表され、TPM1.2自体はオープン仕様で、コストや柔軟性を考慮してハードウェア部分は最小限にし、他の部分はソフトウェアで実現している。また、プラットフォームを利用するソフトウェアとして**図1.3**に示すようなTSS（TCG Software Stack）があり、異なるTPM間の互換性も確保している。これはリソースが制限されたTPM機能を補完するソフトウェアモジュール群である。

ソフトウェアベンダーはこの各APIに準拠したアプリケーションを開発すれば、ソフトウェア間の相互運用性が確保される。また､TPMに準拠した管理ツールも提供されている。TPMに対応したCSP（Cryptographic Service Provider）やMicrosoft社のCrypto-API、RSA Security社のPKCS#11も提供されていて、利用者のI課題としては、TPM内の暗号鍵が物理的に破損した場合の復旧、各社の実装が異なることからくる互換性確保、プラットフォーム認証に係るプラットフォーム保護等がある。

アプリケーション（Microsoft Outlook、Internet Explorer、Adobe Acrobat等）も利用できる。

こうして、従来ソフトウェアで実行されていた鍵の生成・保管・演算機能等が堅牢なハードウェアで実現され、より高いセキュリティ確保が可能となる。

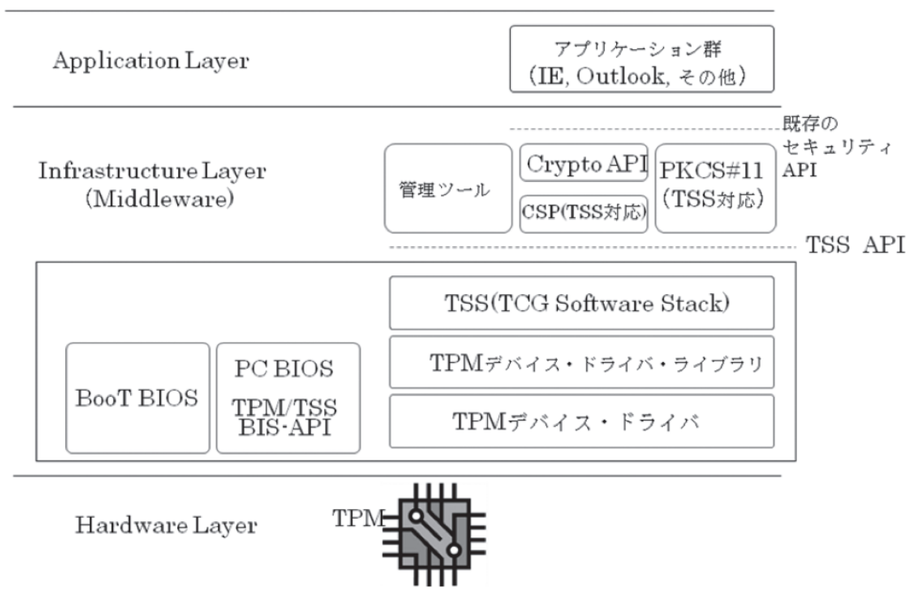


図1.3　TCGのソフトウェア・スタック構成

TPMを使った例としては、IntelのTXT（Trusted eXecution Technology）や、MicrosoftのWindows Vista Enterprise及びUltimateに搭載されたドライブ暗号機能「BitLocker」などがあり、ビジネスユースのPCに幅広く装備されている。今後は仮想化

ソフトとの連携など、様々なアプリケーションと協調しながら普及する可能性がある。（日立ソリューションズの情報セキュリティブログ：http://securityblog.jp/words/487.html　参考）

■参考文献：日本画像情報マネジメント協会報告書「信頼できるコンピューティング環境の実現に向けて～Trusted Platform Module(TPM)の可能性～」2006年3月」
https://cervi.jp/sharess1/jesap.org/tempfiles_JIIMAhoukoku/060328FINAL.pdf

1.2　情報家電 ・ 家庭内制御系　(p.8)

家庭内のネットワークによる制御は、1980年代から多くの方式が提案されているが、国内で実用的に広まったものは無かった。

近年は、DLNA(Digital Living Network Alliance)が家庭内の家電の制御のデファクト ・ スタンダード(事実上の標準)となっている。

DLNAは、UPnP (Universal Plug and Play)を基礎に置いている。

UPnPはUPnPフォーラムが定めたネットワークプロトコルであり、IPプロトコルを使用したネットワークにおいて、ネットワーク機器がお互いを探しあい、認識するためのプロトコルである。UPnPでは、対応したネットワーク機器をネットワークに接続するだけで、自動的に認識され、使用可能になることを目指している。

UPnPフォーラムは、マイクロソフト、インテルなどが参加して立ち上げたが、そのまま実用ネットワークで運用するには、曖昧な要素があった。

そこで、UPnPの応用の一つとして、DLNAが作られた。DLNAはUPnPプロトコルを使用して通信を行う。

DLNAでは、ネットワークに接続する機器を、制御を行うコントローラと、制御される機器(デバイス)に分け、新しく機器やコントローラをネットワークに接続した時に、機器が存在を通知し、認識しあうプロトコルを厳密に定めた。

DLNAにより、IPプロトコルを使用する機器が、自動的に認識されるようになり、情報家電の手軽な制御が実用的になった。

HDDレコーダ、TVやセットトップボックス(STB)、ネットワーク ・ アタッチド ・ ストレージ(NAS)が、DLNAに対応しており、家庭内のネットワークにSTBやNASを接続するだけで、NAS上に格納された動画ファイルを、STBやTVで簡単に再生できるようになっている。

DLNAは、主に、機器がその存在を通知するプロトコルと、制御するプロトコルから成り立つ。

デバイスがネットワークに接続されたとき、自発的に、自分の存在をアドバタイズ(公告)する。その公告はブロードキャストで行われる。

コントローラは、デバイスを発見したら、そのデバイスと通信し、そのデバイスの属性、機能などを取得する。

コントローラは、DLNAプロトコルを使用して、デバイスから動画のリストを取得したり、プレーヤ機能をもったデバイスを制御して動画の再生を行ったりできる。

ユーザはコントローラを操作する。

コントローラは、家電のいわゆるリモコンの形をしている場合もあるが、場合によっては、TVやSTBなどの再生装置が、プレーヤ ・ デバイスと、コントローラの機能の両方を備えている場合もある。その場合、ユーザは、TVと対話し動画リストの取得、動画の選択、再生の制御などを行う。

DLNAは、現在、動画、オーディオ、静止画などを扱う機器でよく使用されている。

DLNAの装置

●デジタルメディアサーバ (DMS)

デジタルメディアレンダラ(DMR)とデジタルメディアプレーヤ(DMP)に向けたコンテンツを格納しておく。PCやNAS。

●デジタルメディアプレーヤ(DMP)

DMS内のコンテンツを見付け、再生とレンダリング(表示、楽音再生)の機能を持つ。TV、ステレオ、ホームシアタ、ゲーム機など

●デジタルメディアレンダラ(DMR)

デジタルメディアコントローラ(DMC)からコンテンツを受け取り再生する。コンテンツはDMSから見つかったものである。TV、AV受信機、ビデオディスプレイや音楽用スピーカ。

●デジタルメディアコントローラ(DMC)

DMS内のコンテンツを見つけ、DMRに再生させる。タブレット型機器、WiFi機能付きデジタル ・ カメラ、PDA。

●デジタルメディアプリンタ(DMPr)

DLNAネットワークで印刷を提供する。一般的に、印刷機能付きのDMPとDMCがDMPrで印刷できる。ネットワーク対応フォトプリンタやオールインワン ・ プリンタ。

■参考URL:

DLNA (Digital Living Network Alliance)
http://www.dlna.org/home

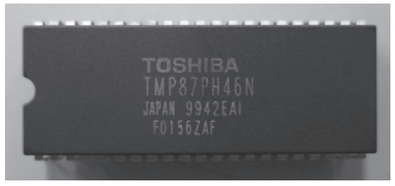
UPnPフォーラム
http://www.upnp.org/

1.3　BGA(ボールグリッドアレー)パッケージ(p.19)

IC部品のパッケージ形状の1種。パッケージ底面に端子が格子状に並べられており、基板実装後は端子から信号を引き出すのが難しい。

ICなどの半導体部品を回路基板に取り付けるには、半導体ダイの端子と回路基板上の端子を接続する必要がある。半導体ダイ上に基板上端子との接続に適したサイズで端子を実装することはできないため、**図1.4**のようなパッケージに半導体ダイを封入し、ダイから端子を引き出して用いる。**図1.5**は、**図1.4**のパッケージ内部を写したX線透過写真である。**図1.5**の中央にある半導体ダイとパッケージ外部の端子が、ボンディングワイヤによって結ばれていることが分かる。

IC部品のパッケージとしては、**図1.4**のようなDIP（Dual Inline Package）が長く用いられてきたが、回路基板の集積度を高める必要から、より小さな面積で多くの端子を持つパッケージが使用され始めている。とくに、表面実装用パッケージとしてSOP（Small Outline Package）、QFP（Quad Flat Package）がある（**図1.6**）。BGAも、これらと同様にICパッケージに実装できる端子数を増やす目的で導入された。DIP、SOP、QFPなどがパッケージ外縁に端子を配置するのに対して、BGAパッケージではパッケージ底面に端子を配置する（**図1.7**）。図のように球状の端子が格子状に配列されることが、ボールグリッドアレー（Ball Grid Array）の名称の由縁である。BGAパッケージ内部では、半導体ダイと端子が**図1.8**のように接続されている。



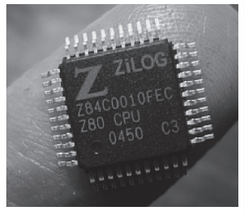
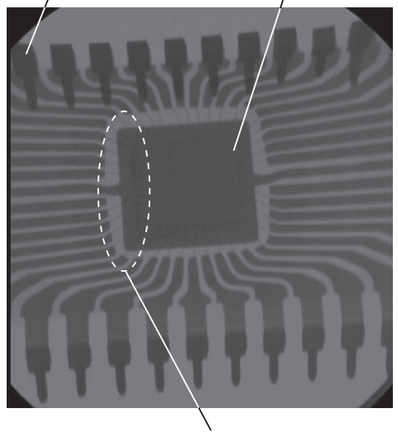


図1.4（上）：半導体パッケージ（DIP）

図1.5（右）： 半導体内部のX線透過写真

図1.6（下）： QFPパッケージの例（Wikipediaより抜粋[1]）



BGAパッケージを回路基板上に実装すると、**図1.9**のようにICの端子がパッケージに隠されて、外部から接触できなくなる。表面実装であるため、はんだ面からICの端子に触れることも難しい。このことは、BGAパッケージの副次的な長所と短所になる。長所は、出荷後の製品から動作時の信号を取り出すことが難しいため、セキュリティの向上につながる点である。この反面、BGAパッケージを製品開発の当初から用いると、デバッグが困難になる。また、手付けが難しいため、製造時にメタルマスクを用意する必要があるなど、製造設備に追加的な投資が必要な場合がある。端子とはんだボールがしっかり融着しているかどうかは目視では確認できないため、製造後の検査や故障解析は、JTAGのような手法によるか、**図1.8**のようなX線透過写真を撮影できるX線装置を用いる必要がある。

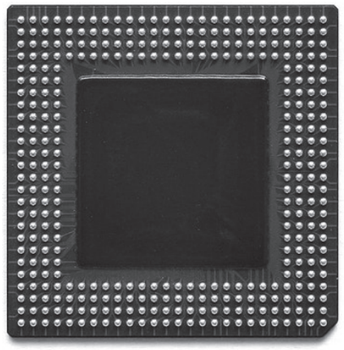
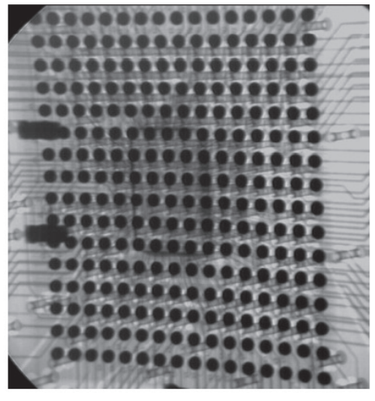
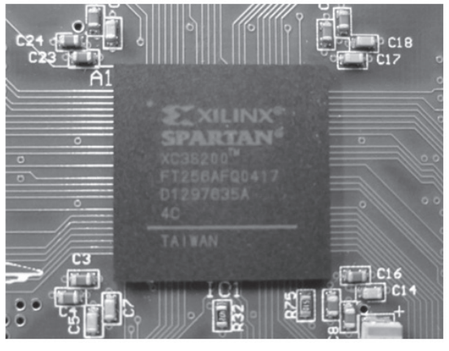


図1.7（左）：BGAパッケージの例（Wikipediaより抜粋[2]）

図1.8（左下）： BGAパッケージ内部のX線透過写真

図1.9（右下）： BGAパッケージの実装例





■参考文献 ：

[1] Wikipedia, “Quad Flat Package,”
http://en.wikipedia.org/wiki/Quad_Flat_Package.
[2] Wikipedia, “Ball grid array,”
http://en.wikipedia.org/wiki/Ball_grid_array.

1.4　開発用のデバッグコネクタ（JTAG）(p.22)

開発用のデバッグコネクタ（JTAG：Joint Test Action Groupの略）[1]-[2]は、集積回路や基板の検査、デバッグなどに使える、バウンダリスキャンテストやテストアクセスポートの標準 IEEE 1149.1の通称である。JTAGは本来この検査方式を定めた業界団体(Joint European Test Action Group)の名称であり、略してJETAGであったが、Europeanが抜けJTAGとなったものである。

開発用のデバッグコネクタ（JTAG）の利用について

開発用のデバッグコネクタ（JTAG）を用いたスキャンテストは、ICチップの製品出荷時に行われる品質検査方式の1つである[3]。スキャンテスト方式は、ICチップに含まれるフリップフロップを数珠状に連結しシフトレジスタを形成して、その両端へアクセスできる端子だけをIC外部に取り出し、IC内部のフリップフロップの状態を少量のピンを用いて検査できるようにしたものである。この数珠上に連結されたフリップフロップをスキャンチェインやスキャンパスなどと呼ぶ。バウンダリスキャンテスト方式は、スキャンテスト方式の一種であり、特にIC外部の入出力ピンの状態を検査するものである。JTAGは、バウンダリスキャンテストの標準方式を定めた団体の名称であり、その規格の通称でもある。JTAG方式では、**図1.10**に示すように、ICチップ内部に各入出力ピンに対応したバウンダリスキャンセルがあらかじめ配置されている。

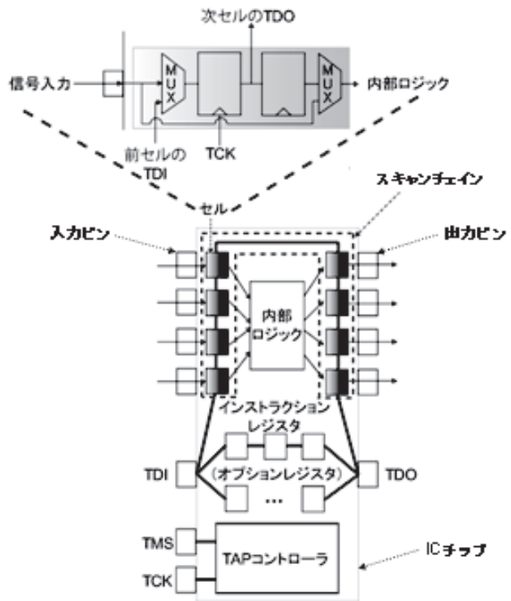


図1.10　JTAGのスキャンチェイン

JTAG方式のテストでは、これらのバウンダリスキャンセルに外部からテストパターンを入力し、その入力に対して期待される出力に問題が無いかを確認する。JTAG方式のテストシステムは、比較的高機能なMPU（Micro Processer Unit）やFPGAのほとんどに内蔵されていて、ICチップ製造時の検査や基板実装後の検査などに利用されている。

JTAG方式のテストを行うためのコントローラは、TAP(Test Access Port)コントローラとして標準化[1]されている。TAPコントローラには、最低でもTDI（Test Data In)、TDO(Test Data Out)、TCK（Test Clock)、TMS（Test Mode Select）の4本の信号線から成る入出力用のシリアルインターフェースがある。TCKは、テスト時にクロックを供給するものである。各バウンダリスキャンセルは、TCKの立ち上がりエッジに同期してTDIから入力される信号を保持し、TCKの立ち下がりエッジでTDOの値を保持する。また、TMSは、テスト動作を制御するものである。

バウンダリスキャンセルは、ICのピンごとに設けられるため、MPUなどのICは、非常に多数のバウンダリスキャンセルを含むスキャンチェインを有する。JTAG方式を用いてすべてのピンの信号値を読み出すためには、セル数分のテストクロックをレジスタに入力する必要がある。

JTAGテストには、ノーマルモードとテストモードの二つの動作モードがある。ノーマルモード動作では、**図1.11**のマルチプレクサ(MUX)がICの外部入出力ピンと内部ロジックを結合するため、バウンダリスキャンセルの存在は内部ロジックから透過的である。このとき、MPUは通常動作を行うが、デバイスのピンを通過する信号はセル内のフリップフロップに保持されるため、MPUの動作に影響を与えないで入出力ピンの状態をスキャンチェインに取り込むことができる。スキャンチェインに取り込まれた信号は、TAPコントローラで受け取ってTDOピンからIC外部に出力し、デバイスの動作状況を観測することが可能である。

テストモード動作は、IC内部ロジックを外部入出力ピンと切り離すため、ICは外部との入出力ができなくなる。したがって、内部ロジックにはテスト信号だけがバウンダリスキャンセルから与えられることになる。ICチップ製造時の検査や基板実装後の検査などにはこのテストモード動作が主として使われている。

またプロセッサのバウンダリスキャンの読み出しには、JTAGノーマルモードのSAMPLE命令を利用する。**図1.11**は、JTAGテストでのSAMPLE命令の動作を示したものである。SAMPLE命令は、CaptureデータレジスタステートとShiftデータレジスタステートの2つのステートからなり、CaptureデータレジスタステートからShiftデータレジスタステートに連続的に遷移する。まずTAPコントローラをCaptureステートに遷移させる。

Captureデータレジスタステートでは、入出力ピンに設定されているデータがスキャンチェインに取り込まれる。次いで、TAPコントローラをShiftステートに遷移させ、スキャンチェインの読み出しを行う。Shiftデータレジスタステートでは、バウンダリスキャンレジスタの内容を1ビットシフトしてTDOから出力すると同時に、TDIから新しいデー

タを1ビット入力する。

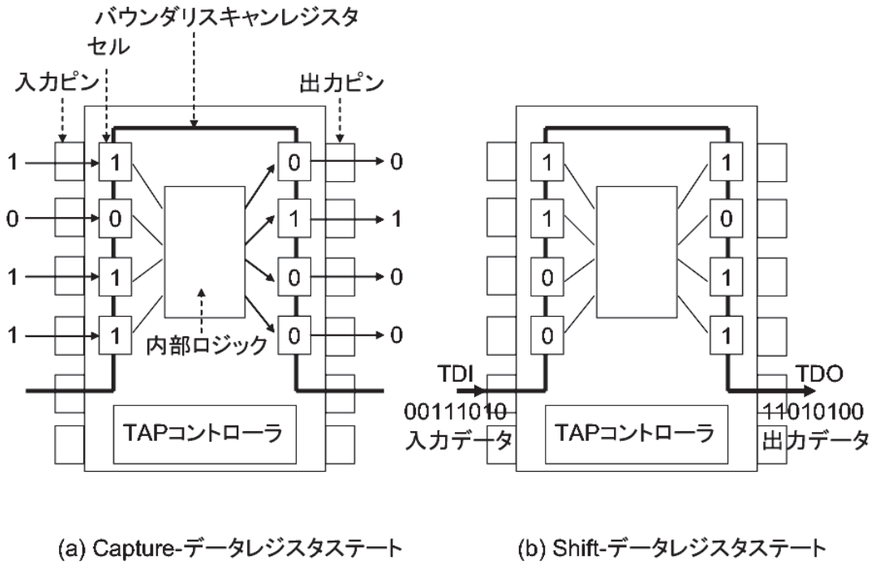


図1.11　JTAGのSAMPLE命令の動作

関連研究について

従来、JTAGを含めたスキャンテスト方式は、IC製品の出荷前品質検査のために用いられてきた。近年のVLSIは非常に多くの入出力ピンや内部フリップフロップを有するため、スキャンチェインを順次シフトしてテストパターンを入力するのは困難になってきた。このため、多くのスキャンテストパターンの改良法や、テストパターンの圧縮法が提案されている[4]-[5]。また、外部からテストパターンを印加せず、IC内部にその生成機構を組み込むBuilt-In Self-Test(BIST)方式の手法も数多く報告されている[6]。従来、ICの通常動作時には利用されていなかったJTAGを、組込みシステムのオンライン監視の目的で利用する手法[7]やコンピュータシステムのオンライン監視手法も多く提案されている[8]-[11]。また、通信の信頼性向上にあたり、省電力化や高速化などの目的で、暗号化機能をFPGA上にハードウェア化する手法が提案されている[12]。

■参考文献：

[1] IEEE Standard Test Access Port and Boundary-Scan Architecture - Description (1990).

[2] 坂巻佳壽美(1998)：JTAGテストの基礎と応用,CQ出版社.

[3] 入月康晴,大原衛,坂巻佳壽美(2008)：“JTAGを用いた組込みシステムのセキュリティ向上に関する一考察”，21回秋季信頼性シンポジウム,pp.9-12.

[4] 米田友洋，梶原誠司，土屋達弘(2005)：ディペンダブルシステム，共立出版.

[5] 宮瀬紘平，梶原誠司(2006)：“レディスダーカ”,Vol.47，No.6，pp.1648-1657.

[6] 佐藤康夫,中尾教伸(2004)：“疑似ランダム論理BISTにおけるテストパターン品質の評価”,電子情報通信学会論文誌D，No.1，pp.35-41.

[7] 入月康晴，大原衛，坂巻佳壽美(2010)：“JTAGを用いた組込みシステムのオンライン自己監視手法”，日本信頼性学会誌,Vol.32,No.3,pp.185-190.

[8] Metra，C.，Favalli，M. and Ricco，B.（2000)：“Self-Checking Detection and Diagnosis of Transient，Delay，and Crosstalk Faults Affecting Bus Lines”，IEEE Trans. Comput.，Vol.49，No.6，pp.560-574.

[9] Usas，A.（1975)：“A Totally Self-Checking Checker Design for the Detection of Errors in Periodic Signals”，IEEE Trans. Comput.，Vol.24，No.5，pp.483-489.

[10] 松本典剛,遠藤浩通,山田勉,中三川哲明,齊藤雅彦(2004)：“遠隔監視向け端末のためのブロック型アーキテクチャの提案と評価”,情報処理学会論文誌,Vol.45,pp.91-99.

[11] 永田和生,原田英雄,牛嶋和行,久我守弘,末吉敏則(2007)：“FPGA遠隔再構成システムの設計と実装”,電子情報通信学会論文誌D，Vol.90-D，No.6，pp.1357-1366.

[12] 堀洋平ほか(2008)：“FPGAの動的部分再構成を用いたマルチ暗号モジュールの回路規模と消費電力の削減”,情報処理学会論文誌ACS,Vol.1，No.2，pp.47-58.

1.5　サービスマン用通信端子　(p.23)

デジタル機器のメンテナンスをするために、メンテナンスツールと接続するための端子で、容易にアクセス出来ないように端子の形状、プロトコルなどを工夫する必要がある。

特に、デジタル複写機、大画面テレビなど大型重量物で修理・メンテナンス作業はメーカーのサービス拠点ではなく使用者の据付け場所で行う事になる。

したがって、サービス拠点とは違い第三者による脅威が大きくなるので、より高度な対策をとることが重要となる。

某社デジタルテレビのケースを次に示す。

「本体前面」にスマートメディア挿入口がある。

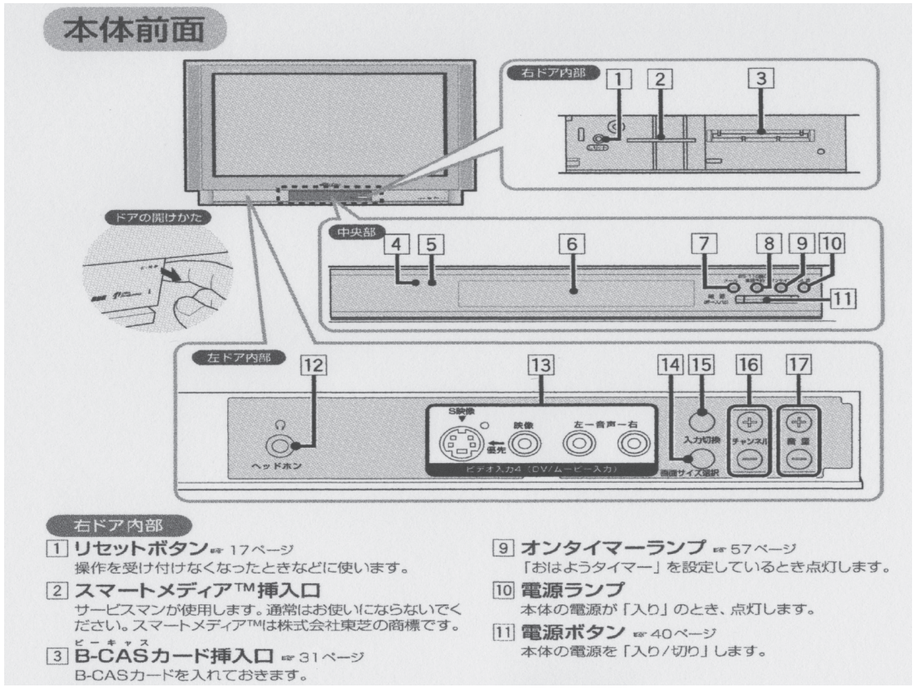
「本体裏面」にシリアル端子（サービス用）がある。

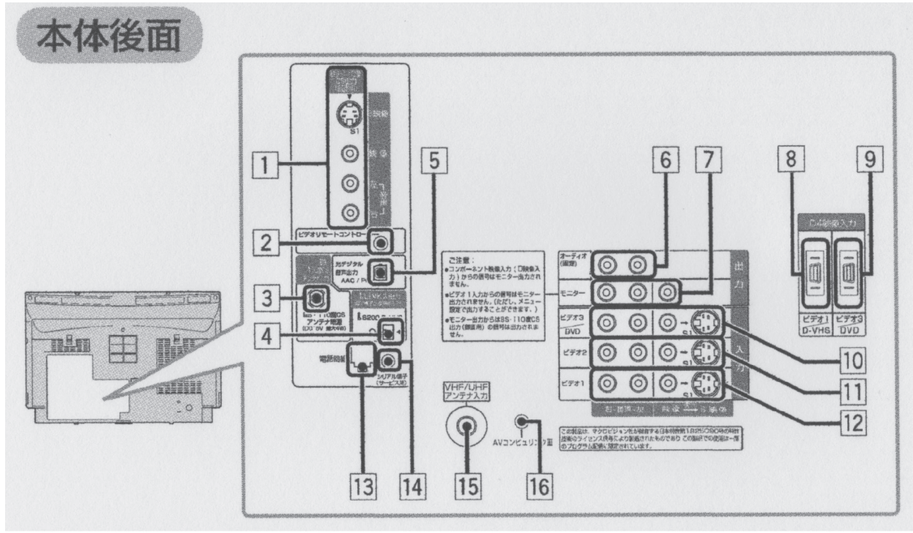
工夫している点：

1．スマートメディアに個人認証用データを入れる事が出来る。

2．接続用端子が、RS-232C、RJE45、USBなどの汎用的なコネクタではない。

3．サービスマンのなりすましの防止、作業ログなどの必要なデータ採取が可能となる。





テレビに映っている映像・音声を出力します。
- BSデジタル放送や110度CSデジタル放送やD4映像入力（ビデオ1、ビデオ3）端子から入力した映像信号は、モニター出力端子からは出力されません。
- 番組一覧中は、モニター出力端子からは出力されません。
- 2画面表示中は、左側の映像と音声が出力されます。

8 ビデオ1/D-VHS:D4映像入力端子 ☞120ページ
D-VHSビデオデッキなどのD端子をもった機器をつなぎます。
- D4映像入力に映像信号が入力されているときは、ビデオ1入力に入力されるS1映像信号や映像信号より優先されます。

14 シリアル端子(サービス用)
サービスマンが使用する端子です。通常は使用しないでください。

15 VHF/UHFアンテナ入力端子 ☞21ページ
VHF、UHFアンテナをつなぎます。

16 AVコンピュリンクIII端子 ☞127ページ
AVコンピュリンク対応の機器をつなぎます。

この他にも接続端子の工夫の例として次のものがある。

某社制御機器の例

1．電気的インターフェースはRS-232C

2．制御機器側コネクタはDSUB-9ピン、メンテナンス機器側はRJ45-8ピン

3．ケーブルの接続図は非公開。

以上の例の他にも、サービスマン用端子は悪意のある第三者から狙われやすいためか、保護するための工夫は多くの例が見られる。

1.6　故障利用攻撃　(p.24)

一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、攻撃者の意図する異常な処理を行わせる攻撃である。

直接物理的な攻撃を与える場合とは異なり、攻撃対象自体を利用できることを前提とする。

秘密鍵を推定する例として暗号処理中に電圧変動などの外乱を与えて一過性の計算誤りを発生させ、出力される異常な演算結果に基づいて秘密鍵を推定する。

故障の誘発には実装アルゴリズムの特定の処理に合わせて、意図した故障をタイミング良く発生させる必要があるため、攻撃の難度は高い。

例 ： 故障利用暗号攻撃によるRC5の解読（抄録）

立情報学研究所論文情報ナビゲータ「サイニィ」より

http://ci.nii.ac.jp/naid/110003251010

Bellcore の Boneh らにより、ICカード等のタンパーフリーデバイスの計算結果の誤りを利用した新しい暗号解読法のアイデアが発表された。

これは公開鍵暗号で用いられているべき乗剰余演算等の代数演算を実装したタンパーフリーデバイスに、放射線や高電圧をかけたり、瞬間的にクロックの周波数を上げたりすることで故意にエラーを起こさせ、その結果誤った計算結果と元の正しい計算結果からそこに格納されている秘密(鍵)情報を得るというものであった。

これを受けてBihamとShamirが同様の仮定のもとで共通鍵暗号が実装されたタンパーフリーデバイスからも鍵を求めることができ、DESに適用した場合、200通りにエラーを起こした暗号文から鍵を求めることができると発表した。

この後も多くの研究者らによりさまざまな条件下での適用例やより現実的な攻撃モデルの提案がなされている。本稿ではこのような攻撃法について考察し、多くのブロック暗号に適用可能ないくつかの現実的な攻撃モデルを整理し図１にした。

またこの攻撃法の適用例として、任意のプロック長、段数、鍵長の各パラメータをもつRC5 の拡大鍵を導く手続きを示し同じく**図1.12**にした。

また、産総研つくばセンターには故障利用攻撃等の設備を備えた設備があり、CC評価にも利用できるようである。

http://www.rcis.aist.go.jp/files/events/2010/0514-ja/RCIS2010_Yamanashi.pdf

http://www.rcis.aist.go.jp/files/events/2010/0514-ja/RCIS2010_Yamanashi.pdf

これらの施設はサイト認証（CC評価に利用できる施設であることの認定）の取得を予定している。

攻撃の分類

システム、モジュールなどに対する故障利用を含め、そのほかの攻撃の分類と種類を**図1.12**に示す。

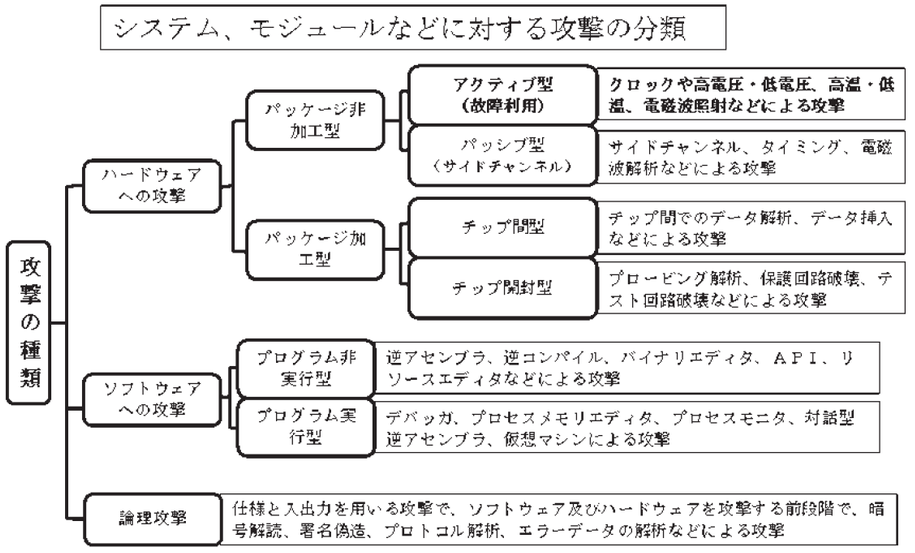


図1.12

1.7　バス暗号化（Bus encryption）（p.26)

バスとは狭義にはコンピュータ内部で各回路がデータをやり取りするための伝送路であり、そこを行き来するデータを保護するため暗号化することをバス暗号化（Bus encryption）という。

1. バス

コンピュータのバスには、大別して（１）CPU内部の回路間を結ぶ内部バス（CPUコアと内蔵キャッシュを接続するバスなど）がこれにあたる、（２）CPUとメモリなどの周辺回路を結ぶ外部バス及び（３）拡張スロットに接続された拡張カードを結びその間でデータをやり取りして拡張カードを機能させる拡張バスの3種類がある。データの伝送は複数の信号線で同時に複数のビットを転送するパラレル転送方式行っており1回の転送で同時に送れるデータの量を「バス幅」と呼ぶ。拡張バスの代表的なものとしてはPCI-Expressなどが有る。**図1.13**にバスの概念の構成例を図示する。

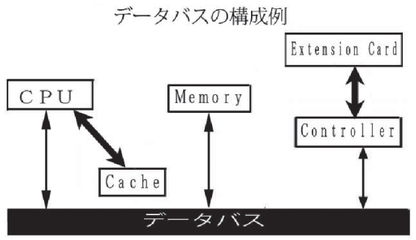


図1.13

2. 暗号

バスの内部を行き来するデータを取り出されて、改ざんされたり、悪用されることから守るため、即ちセキュリティのためには、暗号化するのが一般的である。暗号化、復号化には暗号表に当たる「鍵」を使うが、対になる2つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる秘密鍵暗号に大別される。バスデータに対する主な脅威とそれに対抗する暗号化技術及び代表的な例を**表1.2**にまとめた。

表1.2

脅威の種類	対抗策としての暗号化技術	代表的な例
情報の盗み見	情報を読めない内容にする暗号化技術	共通鍵暗号 公開鍵暗号
情報の改ざん	情報が改ざんされていないことを確認する暗号化技術	ハッシュ関数 電子署名
なりすまし	情報を送った相手を確認する暗号化技術	電子署名

3. PC本体以外の機器の身近なバス暗号化の例

PC用外付けデジタル放送チューナ

身近な例の第一としてPCに外付けするタイプのフルセグ地上デジタル放送チューナおよびＢＳ／ＣＳデジタル放送チューナでの著作権保護のために利用されている暗号化について述べる。

下の参考図のように、TVやセットトップボックスに比べPC はオープンなアーキテクチャであるため、デジタルデータを取り出すことが比較的容易である。

それに対するコンテンツ保護策としてARIB（社団法人 電波産業会）では、“地上デジタルテレビジョン放送運用規定で、保護の対象となるコンテンツを、ユーザーアクセスバスに出力する場合や記録媒体への蓄積を行う場合、ローカル暗号を用いて暗号化することでコンテンツを保護すること、と定めている。その概念を**図1.14**にまとめる。

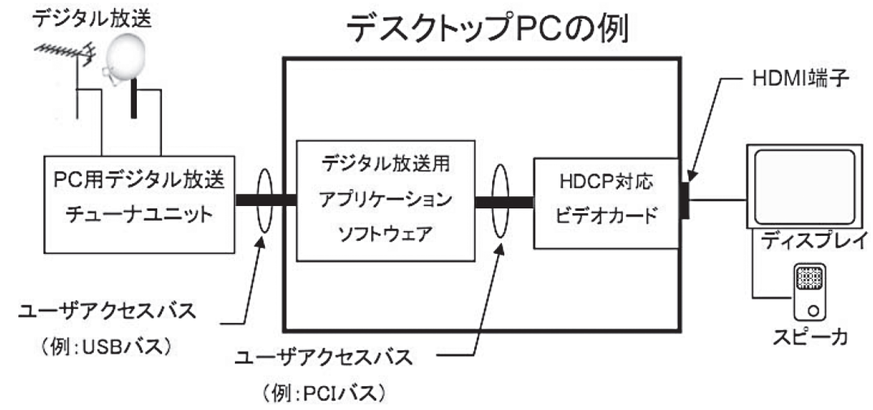


図1.14

以上の出典 ：

(1) AV ノートPCにおける地上デジタル放送アーキテクチャ
http://www.toshiba.co.jp/tech/review/2006/07/61_07pdf/a04.pdf
(2) 社団法人デジタル放送推進協会　PC用デジタル放送チューナのガイドライン
http://www.dpa.or.jp/images/bs/PCtuner-guideline1.0.pdf
(3) ARIB TR-B14 第3分冊 - ARIB 社団法人 電波産業会
http://www.arib.or.jp/english/html/overview/doc/4-TR-B14v3_5-3p3.pdf　より

DVD コンテンツにおける暗号化と複合化の仕組み

CPRM[1] 対応のDVDではコンテンツを保護するため暗号化されている。その仕組みは以下のようになっている。**図1.15**はその概念図である。
PCシステムにおいては、DVDディスクから読み出されたスクランブルコンテンツがハードディスクなどへ不正にコピーされることおよびデコーダモジュールがその不正コピーを再生することを防ぐために、PCシステム用のバス認証が必要になる。

PCシステムにおいては、CSS暗号化されたコンテンツ及び鍵を読み出すDVDドライブとこれらを復号するDVDデコーダとが分離しており、その間の インタフェース上で鍵情報をセキュアに伝送する必要がある。このため、DVDドライブとDVDデコーダはSFF（Small Form Factor Committee）8090規格で定められたプロトコルに従って相互認証を行い、相互認証が成功した場合にのみ鍵情報の伝送を行う。伝送に際しては、相互認証時に共有され、毎回異なる値を取るバス鍵で鍵情報を暗号化している。

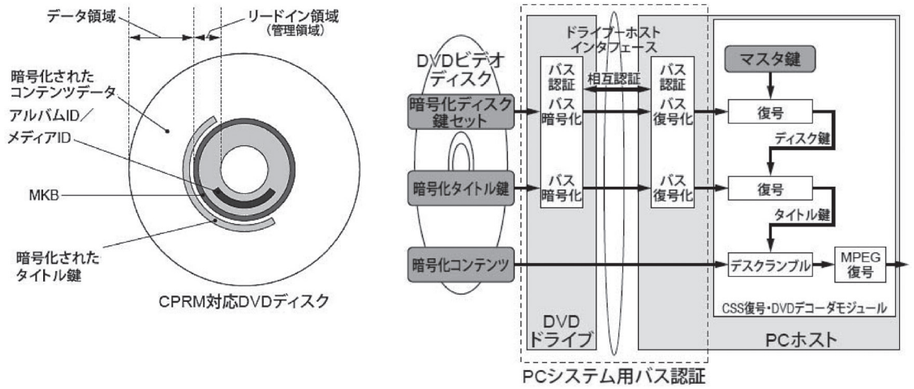


図1.15

出典 ： 石原淳　DVDのコンテンツ保護
http://www.toshiba.co.jp/tech/review/2003/06/58_06pdf/a08.pdf　より

1　CPRM(Content Protection for Recordable Mediaの略、記録メディア向けの著作権保護技術の一つ。デジタルコピーの回数を制限する。

1.8　リバースエンジニアリング攻撃　(p.29)

製品を分解するなどして製品の内部構成を解析し、セキュリティ上の攻撃方法を発見、利用する手法。ソフトウェアをデコンパイルするなどの解析手法についても、この用語が用いられることがある。

リバースエンジニアリング攻撃は、市場に流通している製品をリバースエンジニアリングする（内部を解析する）ことによって、セキュリティ上の攻撃方法を発見するような手法を総称して言う。狭義には、破壊型解析の一分類として、ICチップを観察してセキュリティに関する情報を得る手法を指す場合もある[1]。

多くの組込み製品は、その内部構造を明らかにしていない。ハードウェアの設計図である回路図や、ソフトウェアのソースコードは、企業の知的財産として保護されていることが多い。しかし、これらが公開されていないことは、ただちにセキュリティの向上につながるものではない。リバースエンジニアリングによってその回路やソフトウェアの構造が明らかにされれば、セキュリティを確保するための機構が回避される可能性がある。たとえば、**図1.16**のようにプロセッサとセキュリティ機能を提供するTPM（TPMの項参照）が回路基板上に露出した配線で結ばれている場合、この配線を特定し、これを中途で切断して別途用意した不正なモジュールに繋ぎかえることによって、製品のセキュリティ機能をバイパスできる可能性がある。また、配線がICチップ外に露出していない場合でも、ICチップのパッケージを破壊して内部に直接する攻撃も報告されている。このため、ICチップ製造時には、このような攻撃を想定した耐タンパ性を持たせることが求められる場合がある[2]。

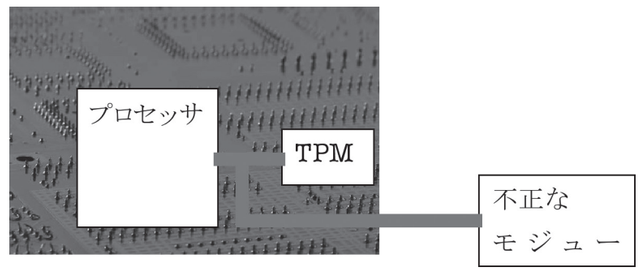


図1.16　不正なモジュールの接続

製品開発時にだけ使用するデバッグ用コネクタが出荷後に残されていたり、サービスマン用の端子に一般のユーザがアクセスできたりすると、より簡単にリバースエンジニアリングが可能になる。製品保守上の理由などによって、製品にこれらの端子を搭載する場合には、デバッグ機能の利用に先んじて認証を行うなどの工夫をして、リバースエンジニア

リングを困難にすることが望ましい。

ソフトウェアのリバースエンジニアリングは、ソフトウェアが動作するプロセッサの技術資料が入手できる場合は、比較的容易である。ソフトウェアを逆アセンブルするなどして、その動作を詳細に知ることができる。このようなリバースエンジニアリングを困難にするために、難読化などの対策が行われる。ただし、他者が作成したソフトウェアを製品に組み込む場合、そのライセンス形態によってはソースコードの公開等が義務付けられる場合がある[3]。

組込み製品の場合、そのソフトウェアは回路基板上のフラッシュメモリに格納される場合が多い。このソフトウェアが外部から不正に読み出されることを防げれば、ソフトウェアの解析を難しくすることができる。このために、暗号化したソフトウェアをフラッシュメモリに格納しておき、これを実行時にプロセッサ内部で復号できるシステムも存在する[4]。

■参考文献

[1] 社団法人ビジネス機械 ・ 情報システム産業協会 論文データベース
http://www.jbmia.or.jp/~card/sec_bunkakai/db/index.html

[2] 電子商取引安全技術研究組合、「システムLSIチップのセキュリティ評価」に関する調査研究報告書、平成16年3月.

[3] GNU, GNU General Public Licence, http://www.gnu.org/licenses/gpl.html.

[4] ALTERA, Protecting the FPGA Design From Common Threats,
http://www.altera.co.jp/literature/wp/wp-01111-anti-tamper.pdf.

1.9 装置ベンダー固有のコード (p.38)

一般には「ベンダー ・ コード(vendor code)」と呼ばれている製造メーカの識別符号。IPv4ではMACアドレスが重複しないよう、上位24ビットにNICメーカ固有の番号を割り当て、下位24ビットはメーカの管理とした。この思想はIPv6やBluetoothにも取り入れられたが、特にDHCPv6ではIPアドレスの決定にもベンダー ・ コードが使用される場合があり、インターネット上から接続機器を特定される可能性がある。

イーサネット上でフレームを送受信する際に使用されるMAC (medium access control)アドレスは、IPv4の場合上位24ビットのベンダー ・ コードと、機器毎に付与された下位24ビットの計48ビットで構成されている。イーサネットアドレスの特殊ビットについての説明は「**図 1.17** イーサネットとIEEE802.3 送信元/宛先アドレスフィールド」を参照のこと。

2バイトフィールド(IEEE 802.3).

16ビットアドレスフィールド	
I/G *	15アドレスビット

6バイトフィールド(イーサネットとIEEE 802.3).

48ビットアドレスフィールド		
I/G *	U/L	46アドレスビット

I/Gビット サブフィールド	'0'=個別アドレス
	'1'=グループアドレス
U/Lビット サブフィールド	'0'=普通管理アドレッシング
	'1'=局所管理アドレッシング
*	ソースアドレスフィールドに 0がセットされる

図1.17 イーサネットとIEEE802.3 送信元/宛先アドレスフィールド

なおイーサネット上でMACアドレスが重複するとネットワーク全体の通信に重篤な支障をきたす恐れがある。そのためベンダー・コードは、イーサネットを標準化したIEEE（Institute of Electrical and Electronics Engineers）によって厳密に管理されており、その情報はweb上に公開[2]されている。

IPv4環境においては、物理的な境界によってイーサネット上のアドレスは遮蔽され、ベンダー・コードの露出を免れていた。ところがIPv6環境ではインターネット上のアドレスにベンダー・コードが反映される可能性があり、接続相手に機器情報を推察されてしまう可能性がある。具体的にはDHCPv6[3]によりアドレスを配布される場合である。

DHCPv6ではアドレス決定に際して、次の何れかが使用される。

①IANA（Internet Assigned Numbers Authority）で保持されたベンダーの登録されたエンタープライズ番号

②リンクレイヤアドレス

何れの場合においても、インターネットアドレス生成の際にサーバおよびクライアントのお互いの識別子として機器の固有情報が使用されるため、攻撃者が特定の機器の脆弱性をついた攻撃を行う際の参考情報として利用される可能性がある。

■参考文献

●組込システム向けTCP/IP IPv6オプションプロトコルスタックDHCPv6(Dynamic Host Configuration Protocol Version 6)Clientユーザーズマニュアル、第1版、図研エルミック株式会社

●組込みシステム開発専用 TCP/IP プロトコルスタック KASAGO TCP/IP ユーザーズマニュアル、第7版、図研エルミック株式会社

【参考URL】

●RFC3315の原文 : http://www.ietf.org/rfc/rfc3315.txt

2 下記のサイトで会社ID/OUI 取得に関する情報が入手可能。
http://standards.ieee.org/faqs/OUI.html.

3 RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

1.10 物理的消去機能 （p.42）

個人情報等の流失を防止するため、記憶装置や記憶媒体の廃棄前に、記憶されている情報を恒久的に読み出せないよう消去する機能。記憶装置自体を物理的に破壊することが多い。

パソコンや携帯電話には、多くの個人情報が保存されていることが多い。これらの機器を廃棄する際には、個人情報の流出を防ぐため確実に情報を消去する必要がある。また、企業などの組織が業務に用いるパソコンやデジタル複合機（MFP: Multi Function Printer）[1]を廃棄する場合や、リース契約満了などによって返却する場合にも同様の配慮が求められる。

これらの情報は、通常はデータファイルとしてOSに管理され、記憶媒体に保存される。このため、OSの機能を用いてこれらのファイルを削除することで、論理的にはデータの消去が可能である。しかしながら、ファイルが論理的に削除されても、HDDやCD、DVD、USBフラッシュメモリなどには磁気や色素、電荷などの物理的な形で情報が残留する。このように物理的に記憶された情報を消去しなければ、記憶媒体から情報を取り出すことが原理的には可能であり、機器廃棄後の情報流出の可能性が存在する。

物理的に記憶された情報を消去することは、一般に容易ではない。たとえば、磁気によって情報を記憶するHDDの場合、フォーマットなどの操作を行ってすべての情報を上書きしたとしても、残留磁気を読み取ることによって情報を再生可能な場合がある。このため、複数回の上書き処理を行い、元の情報が読み取れないほどに残留磁気を弱めるための標準的な方法が、米国防総省などによって定められている[2]。

これらの消去方法の一部は、さらに記憶媒体を物理的に破壊して、読み取れないようにすることを求めている。これには、**図1.18**のような装置を用いる。また、CD-RやDVD-Rなどの一度だけしか書き込めない記録媒体の破壊には、**図1.19**のようなメディアシュレッダー（粉砕機）がよく用いられる。

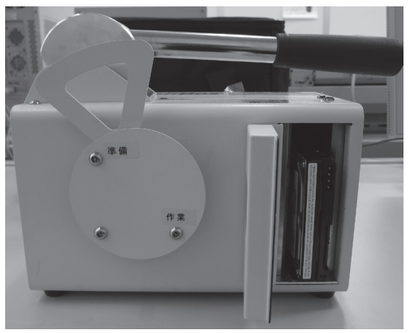


図1.18 HDDを物理的に破壊する装置

図1.19 メディアシュレッダー

近年よく利用されるフラッシュメモリやSSDのような記憶媒体は、消去と記憶を繰り返すと媒体が劣化する特性がある。多くの用途では、一部のファイルに対して集中的に読み書きが行われる局所性が見られるため、このように集中的に書き換えられるファイルをフラッシュメモリなどの同じ領域に固定して記憶すると、その領域の劣化が著しく早く進む可能性がある。このため、多くの機器では、書き込みが行われる度にファイルの物理的な格納領域を変更するウェア・レベリング（Wear leveling）が行われる。ウェア・レベリングが行われる機器では、書き込みが行われる物理的な領域が一定しないため、文献[1]のような方法で情報を消去することが難しい。これらの記憶媒体の消去には、物理的破壊による方法を併用することが好ましい。フラッシュメモリなどは、とくに携帯電話や個人情報端末などでよく用いられているため、これらの端末を物理的に破壊する装置やサービスも販売されている。

■参考文献

[1] IPA、「MFP（デジタル複合機）の脆弱性に関する調査報告書」、2010年8月.

[2] NIST, “Special Publication 800-88: Guidelines for Media Sanitization,” Sept. 2006.

1.11　追加ハードウェア関連キーワード

耐タンパ

モジュールがあらかじめ準備したインタフェース以外のアクセス手段を用いて、許可なくモジュールの内部情報を読み取ろうとする攻撃に対する耐性を指す。耐タンパ実装は、筐体の不正なこじ開け、基板上のデバイスへの不正なアクセス、プロービング、不揮発性メモリのデータの書換え等組込みシステムのハードウェアへの直接的な攻撃に対して耐タンパ機能を実装する技術である。（参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞http://www.ipa.go.jp/security/fy http://www.ipa.go.jp/security/fy22/reports/emb_app2010/emb_guide_fy22.pdf

サイドチャネル攻撃

ICチップが暗号処理を行う際の電力解析（power analysis)、タイミング解析（timing analysis)、故障利用（fault induction）等のサイドチャネル情報（設計者が予想しなかった情報）を用いた攻撃の総称をサイドチャネル攻撃という。漏洩（リーク）してくる情報を解析するので、リーク情報解析攻撃とも呼ばれ、CC（Common Criteria）などでは、別名隠れチャネル（covert channel）攻撃とも呼ばれる。（2003年度経済産業省委託調査研究報告書「システムLSIチップのセキュリティ評価」参照）

暗号モジュール試験および認証制度(JCMVP)

独立行政法人　情報処理推進機構（IPA）が運用している「暗号モジュール試験及び認証制度」のこと。「Japan Cryptographic Module Validation Program」の略で、製品認証の評価制度の一つとして、2007年4月より正式運用を開始している。暗号化機能や署名機能等が、ソフトウエア、ハードウエア等の暗号モジュールに対して正しく実装されていて、その中に含まれる鍵やID、パスワード等の機密情報のセキュリティが確保されていることを試験、認証する制度。組込みシステムのセキュリティへの取り組みガイドの企画・開発方針におけるセキュリティへの取組み「レベル4」に相当する。この水準では、問題が起きた場合に形式的に原因の調査と報告が行えるため、迅速に問題の解決が可能となる。（参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞及びHitachi Solutions情報セキュリティブログhttp://securityblog.jp/words/566.html）

物理的または化学的なマスク処理

デバイス実装後の基板上に感光材や金属層などのパターンを物理的または化学的に焼きつけるマスク処理を行い、プロービングなどに対する耐タンパ性を高める技術。電源投入時にこのパターンに光や断線・ショートが検出されると、攻撃を受けたものとして自己破壊信号を送出する仕組みになっている。

プローブ攻撃

LSIのパッケージを開封し、チップ表面のデータバスに探針（プローブ）を当て、回路を動作させながらバス上のビットの変化を観察することによる解析結果を使った攻撃方法。

プローブ攻撃を防ぐため、機密情報を処理するLSIは外部から動作を観測することを妨げるような保護層を備えたものを使用する。また、回路を取り囲むように金属層を設け、そこに流れる電流をモニタした上で異常を検出した場合には機密情報を破壊する方法や、保護層を取り除こうとするとチップ自体が破壊されるようにする（耐タンパメカニズム）方法もある。（参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞表 4-1 代表的なサイドチャネル攻撃の例）

プロービング

プロービングとは、プローブ（探針）を回路に当ててデータの読み取りやデータの注入を行うこと。データを測定する箇所にプルーブを当てることで、基板上のデータバス上に機密情報が非暗号化された状態で流れる場合には、プロービング等によって攻撃者に盗み取られるといった物理的な攻撃事例がある。この対策には、機密情報を扱う組込みシステ

ムのハードウェアは、筐体の不正なこじ開け防止やBGAパッケージのデバイスを選択するなど、形状を工夫することでプロービングを防止する。

電力解析攻撃

タイミング攻撃と同様に、暗号回路が消費する電力を解析することにより、暗号そのものを解読して内部の機密情報を推定しようとするもの。サイドチャネルアタックの一種だが、単純電力解析（SPA）や、電力差分解析（DPA）といった、様々なバリエーションが検討されている。（参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞表 4-1 代表的なサイドチャネル攻撃の例）

単純電力解析（SPA ： Simple Power Analysis）攻撃

SPAは、最も基本となる電力解析攻撃の一つであり、暗号処理中の電力波形から直接秘密情報を推測する手法。暗号アルゴリズムの特徴及び実装、暗号モジュールの電気的な消費電力の変化を監視して秘密情報を導出する。

電力差分解析（DPA ： Differential Power Analysis）攻撃

多数の消費電流波形に対して統計的処理を行うことで暗号鍵を推定する方法。消費電流波形の解析は、DES 暗号の場合は置換時の波形とシフト時の波形の差、RSA暗号の場合は乗算時の波形と2乗演算時の波形の差を主な着目点としている。

電磁波解析攻撃

LSIの周辺にコイルを近づけ、漏洩している電磁波放射を測定して動作を推測する手法である。得られたサイドチャネル情報が電磁波か電力かの違いがあるだけであるため、その解析手法は電力のそれと同一で、単純電磁波解析(SEMA: Simple Electro Magnetic Analysis）、差分電磁波解析(DEMA: Differential Electro Magnetic Analysis）、そして相関電磁波解析（ CEMA: Correlation Electro Magnetic Analysis）に3分類される。(「SASEBO-R を使用した電磁波解析と電力解析の比較」FIT2009（第8回情報科学技術フォーラム）参照）対策としては、電力解析攻撃、電磁波解析攻撃とも、タイミング攻撃の対策と同様に、演算内容により差異が生じないようにする。(参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞表 4-1 代表的なサイドチャネル攻撃の例)

故障利用攻撃

人為的に暗号モジュール内に故障を起こさせた状態で処理を行わせ、その結果から機密情報を推定する手法である。故障を引き起こすには、定格外電圧や、定格外のクロック周波数を印加する方法や、電磁波、温度限界、及び電圧の不正操作のような外部的な力を活用する。故障利用攻撃を防ぐためには、故障の状態を検知する仕組みを設け、故障を検出した場合には機密情報を破壊する。(参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞表 4-1 代表的なサイドチャネル攻撃の例)

タイミング攻撃

暗号アルゴリズムまたは暗号処理に関係する特定の数学的操作を実行するために必要な暗号モジュールの実行時間を正確に測定することにより、その機密情報を推定する方法である。例えば、モンゴメリ乗算を行う際に、演算の最後の段階で中間結果の値によって、時間がかかる剰余算を行う場合と、行わない場合に分けられる。このため、入力データを変更しながらモンゴメリ乗算行い、その実行時間を測定することで、内部の機密情報が推定できることがある。タイミング攻撃を防ぐためには、演算アルゴリズムにダミールーチンを挿入し、演算内容により差異が生じないようにする。

（LSIの）保護層

機密情報を処理するLSIは、プローブ攻撃などサイドチャネル（設計者が意図しないチャネル）からの攻撃を防ぐため、外部から動作を観測することを妨げるような樹脂や化学物資等をコーティングすることで保護層を備えたものを使用する。また、保護層を取り除こうとするとチップ自体が破壊されるようにする（耐タンパメカニズム）方法もある。保護層は、セキュリティ上の観点のみならず、外部環境からの湿気等の影響による劣化を防ぎ、半導体素子の表面を安定化させる役目もある。(参考 ： IPA「組込みシステムのセキュリティへの取り組みガイド」＜2010年9月改訂版＞)

IPv6（Internet Protocol Version 6）特有のアドレス付与方式

IPv4のアドレス空間の不足、移動通信やセキュリティ対策といった機能の不足に対応するために定義された新しいインターネットプロトコル。IPv4のアドレス長が32ビットであるのに対して、IPv6では4倍の128ビットとなり、提供されるアドレス空間はIPv4の2の96乗倍という広大さとなる。これは、事実上無限と考えてよい。そのほかにも、セキュリティ強化のためIPsecを標準機能とし、アドレスの集約化のために階層的にアドレスを割り当て可能とし、IP拡張ヘッダの形式を統一するなど機能増強を図っている。

UTM (Unified Threat Management) 装置

UTMとは統合脅威管理装置で、ファイアウォール、アンチウイルス、アンチスパム、不正侵入対策などの複数のセキュリティ機能を統合的に管理する機器のこと。一般に「統合セキュリティアプライアンス」と呼ばれる。ファイアウォール、アンチウイルス、アンチスパム、不正侵入対策などのセキュリティ機能が統合された機器のこと。UTMは、複数のセキュリティ機能が一台に搭載されているため、ネットワークの入り口にUTMを接続する

ことで、そこに接続されるすべてのPC、ネットワークに対し、一元的にセキュリティ対策をすることが可能になる。

NSAが定義する消去方法

米国の国家安全保障局（NSA：National Security Agency）は、通信傍受・盗聴・暗号解読などの「国家安全保障」を担当する国防総省傘下の情報機関で1952年に発足した組織。データの消去に関する米国国家安全保障局推奨方式は、米国国防総省DoD5220.22-M（E）規格と呼ばれ、（1サイクル目：1書き込み、2サイクル目：0書き込み）×3回＝6回、7回目に政府指定コード”245”（0xF6）を全ドライブに書き込み、合計7回の書き込みで消去を行う方式である。（参考：Applied Direct「パソコンデータ完全消去サービス」の出張サービス料金表）http://121ware.com/e-manual/m/nx/ma/200605/pdf/pg/sw/v1/mst/ap64/hdclear.htm

微細プロセスのセル

微細プロセスとは、IC構造の微細化を進めるに当たって、ICチップの微細化を実現するプ製造プロセスである。セルとは、ソニー、東芝、IBM社の3社が共同開発したマイクロプロセッサのこと。 ソニー・コンピュータエンタテインメントの家庭用ゲーム機「プレイステーション3」（PS3）へ搭載されている。PS3以外にもIBMサーバや組込み製品、例えば液晶テレビやHDレコーダーなど、様々な電子機器に組み込み可能なCPUである。

物理的または化学的なマスク処理

デバイス実装後の基板上に感光材や金属層などのパターンを物理的または化学的に焼きつけるマスク処理を行い、プロービングなどに対する耐タンパ性を高める技術。電源投入時にこのパターンに光や断線・ショートなどが検出されると、攻撃を受けたものとして扱い、自己破壊信号を送出する仕組みになっている。

情報家電そのものに関する情報

機種、ID（Identification ）、シリアル番号等の機器情報のことで、個々の機器を認証するための情報。従来のMAC（Media Access Control address）アドレスも、ネットワーク上で、各ノードの情報家電を含むネットワーク機器を識別するための物理アドレスである。

Windows Embedded

マイクロソフトが1996年11月以来提供している、Windows Embedded CEをはじめとする組込みOSシリーズのこと。これにより、開発者はモバイルデバイスを始めとする組込み機器、更には次世代の32ビット デバイスに至るまで構築できるようになっている。

第2章
情報セキュリティに関する開発技術や管理についてのアンケート（2010年度）の集計

2011年1月31日までの期間で、JASA会員の全企業に対し表記アンケートを実施し、その結果をまとめ、考察したので報告する。

年初でありご多忙な中にも関わらず、多くの回答をいただいた会員企業の皆様には、厚く御礼申し上げたい。

2.1　アンケート結果についての概要

全フェーズにおいて実施レベルおよび2年以内に実施するレベルともに、レベル3以下となっており、情報セキュリティに対する取り組みが今一歩足りない結果となった。

JASA会員企業は受託開発の比率が多いためか、セキュリティに関しての取り組みレベルは比較的低く、今後はレベルの向上を促す必要があると思われる。

このようなことから、セキュリティワーキンググループとしてはJASA会員企業を中心に情報セキュリティの重要性と具体な対応策について提案をすすめていきたい。

明文化レベルは全体的に2以下となっており、企業内での取り組みに対する標準化を進めることが必要ではないだろうか。

マネジメントフェーズと企画フェーズが現状と2年以内実施ともに上位1・2となっており、開発フェーズの前手順が重要視されていることがわかる。

また、廃棄フェーズは自社商品を持つ企業が少ないこともあって最低レベルを示している。

詳細は次頁以降の、表とグラフを参照頂きたい。

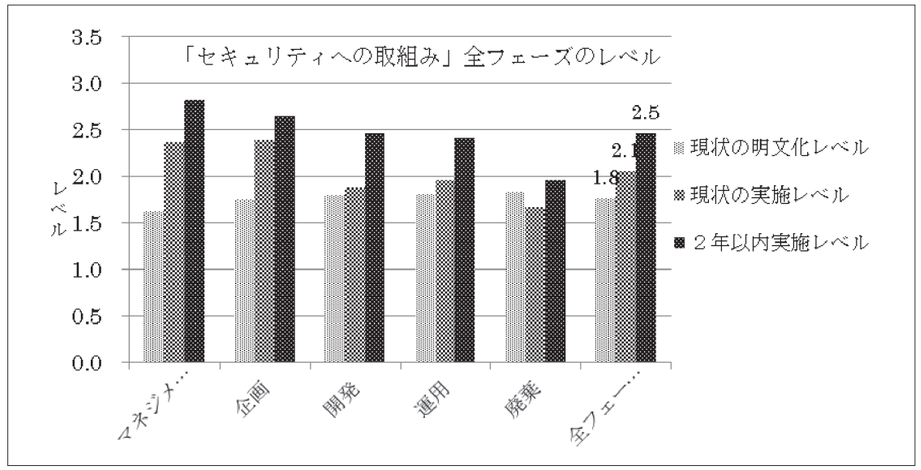
また、回答の中で設問の意図が不明などのご意見を頂戴しており、今後のアンケートをお願いするときには、十分な配慮が必要であることを改めて教えて頂き、回答いただいた企業にはお礼を申し述べたい。

2.7にあるIPAのアンケート結果では、 IPAは情報セキュリティについて各種の施策を行っているが、それに対して「知らない」が30%を超えている。

これらの施策は、組込みシステム開発業界にとって有益なものなので、この結果をIPAに報告するとともに周知方法の見直しを申し入れたい。

表2.1

「セキュリティへの取組み」のレベルとその内容	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
マネジメントフェーズの平均レベル	1.6	2.4	2.8
企画フェーズの平均レベル	1.8	2.4	2.6
開発フェーズの平均レベル	1.8	1.9	2.5
運用フェーズの平均レベル	1.8	2.0	2.4
廃棄フェーズの平均レベル	1.8	1.7	2.0
全フェーズ平均レベル	1.8	2.1	2.5



グラフ2.1

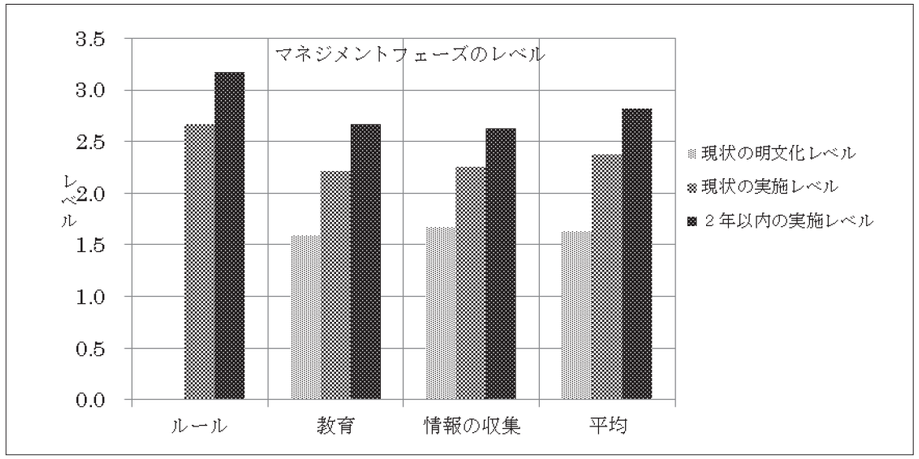
2.2 マネジメントフェーズ

セキュリティルールの２年以内実施が3.2となっており、ルールを確実にする意図が強くあり、今後の取り組みが期待できる。

また、セキュリティ教育についての必要性を認識しているので、今後の施策の検討が必要であろう。

表2.2

セキュリティを考慮すべき項目	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
セキュリティルール		2.7	3.2
セキュリティ教育	1.6	2.2	2.7
セキュリティ情報の収集	1.7	2.3	2.6
平均レベル	1.6	2.4	2.8

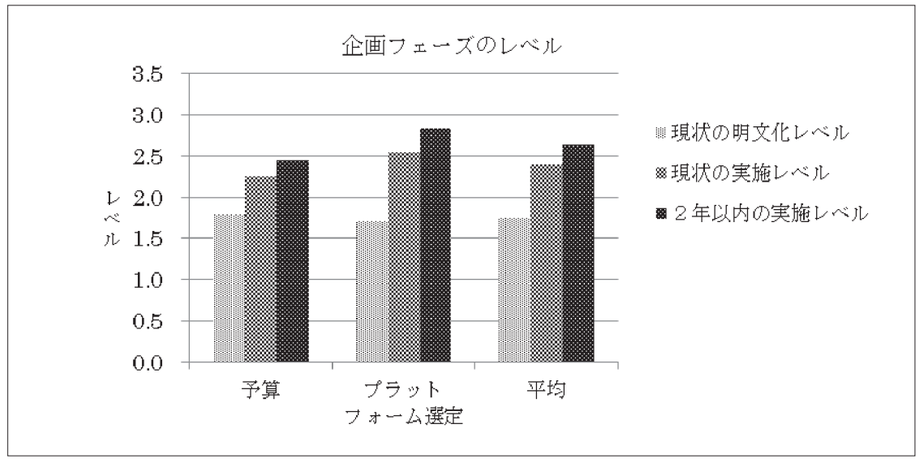


グラフ2.2

2.3　企画フェーズ

表2.3

セキュリティを考慮すべき項目	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
予算	1.8	2.3	2.5
開発プラットフォーム選定	1.7	2.5	2.8
平均レベル	1.8	2.4	2.6

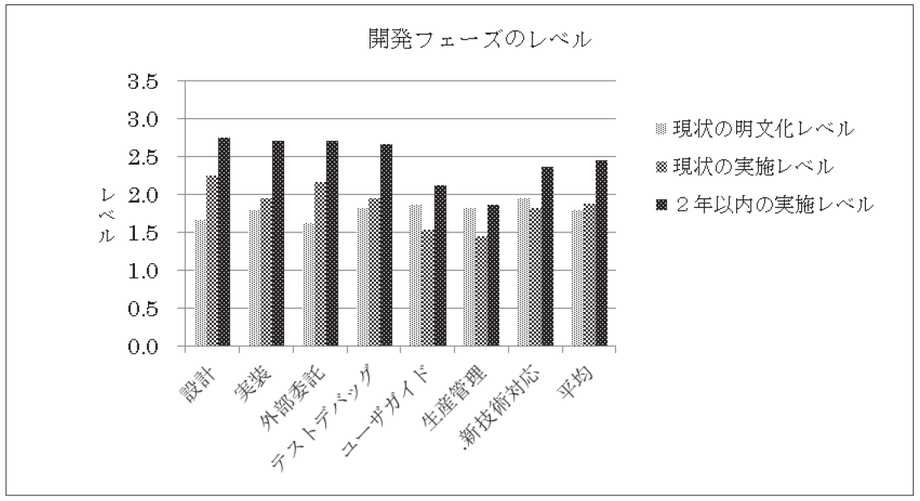


グラフ2.3

2.4　開発フェーズ

表2.4

セキュリティを考慮すべき項目	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
設計	1.7	2.3	2.8
ソフトウェア実装	1.8	2.0	2.7
開発の外部委託における取組み	1.6	2.2	2.7
セキュリティ評価テスト・デバッグ	1.8	2	2.7
ユーザガイド	1.9	1.5	2.1
工場生産管理	1.8	1.5	1.9
新技術への対応	2.0	1.8	2.4
平均レベル	1.8	1.9	2.5

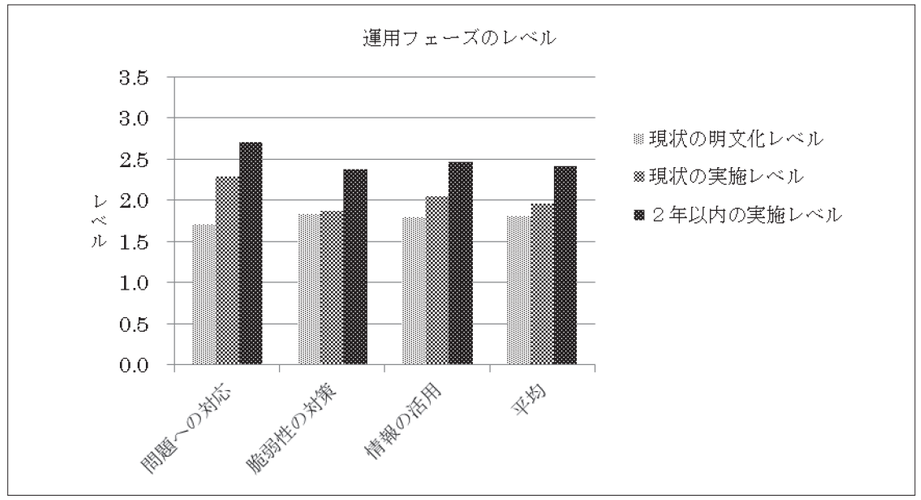


グラフ2.4

2.5　運用フェーズ

表2.5

セキュリティを考慮すべき項目	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
セキュリティ上の問題への対応	1.7	2.3	2.7
ユーザまたは発注者への脆弱性の通知方法と対策方法	1.8	1.9	2.4
脆弱性情報の活用	1.8	2.0	2.5
平均レベル	1.8	2.0	2.4

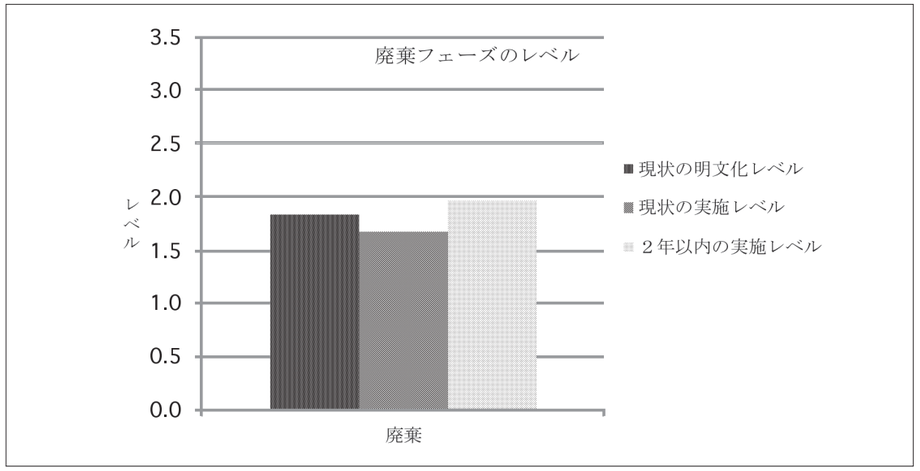


グラフ2.5

2.6　廃棄フェーズ

表2.6

セキュリティを考慮すべき項目	現状のレベル		２年以内に実施するレベル
	明文化レベル	実施レベル	
機器廃棄方法の周知	1.8	1.7	2.0



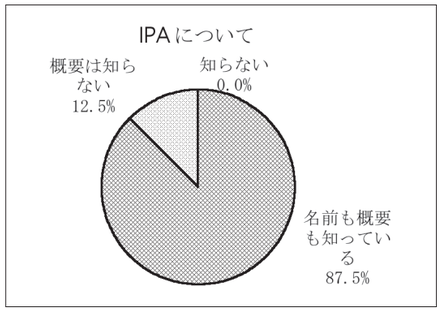
グラフ2.6

2.7　IPAについてのアンケート

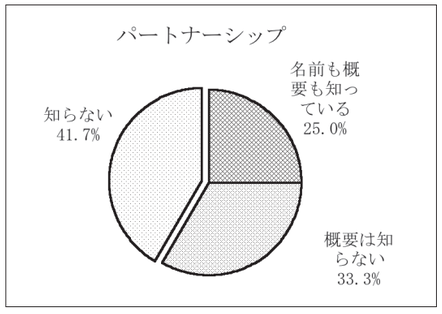
2.7.1　IPAや「情報セキュリティ早期警戒パートナーシップ」の枠組みや活動について

表2.7

IPAや「情報セキュリティ早期警戒パートナーシップ」の枠組みや活動について		%
1. IPA(独立行政法人 情報処理推進機構)について	1. 名前も概要も知っている	87.5%
	2. 概要は知らない	12.5%
	3. 知らない	0.0%
2. 情報セキュリティ早期警戒パートナーシップについて	1. 名前も概要も知っている	25.0%
	2. 概要は知らない	33.3%
	3. 知らない	41.7%



グラフ2.7　IPAについて

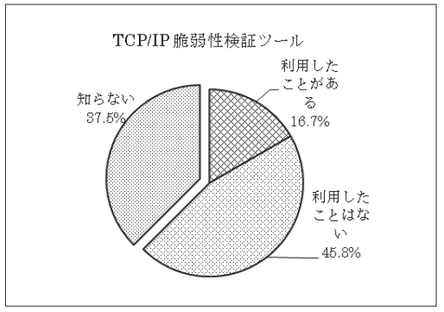


グラフ2.8　パートナーシップ

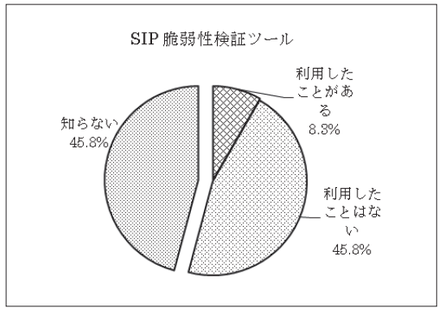
2.7.2　IPAが実施している「TCP/IP脆弱性検証ツール」と、「SIP脆弱性検証ツール」について、貴社における利用状況に当てはまるものは

表2.8

IPAが実施している下記のセキュリティ事業のうち、貴社における利用状況に当てはまるものは		%
1. TCP/IP脆弱性検証ツール	1. 利用したことがある	16.7%
	2. 利用したことはない	45.8%
	3. 知らない	37.5%
2. SIP脆弱性検証ツール	1. 利用したことがある	8.3%
	2. 利用したことはない	45.8%
	3. 知らない	45.8%



グラフ2.9　TCP/IP脆弱性検証ツール

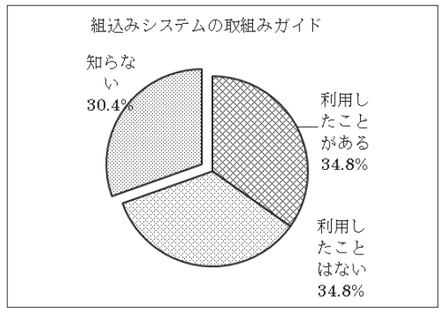


グラフ2.10　SIP脆弱性検証

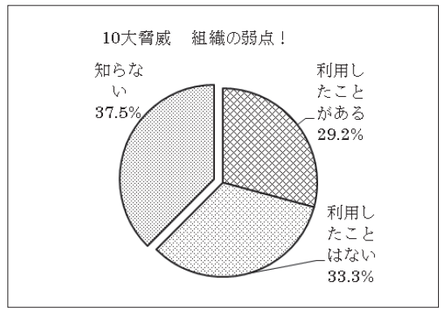
2.7.3　IPAが実施している普及啓発資料「組込みシステムのセキュリティへの取組みガイド」と、報告書「10大脅威 あぶりだされる組織の弱点！」について、貴社における利用状況は

表2.9

IPAが実施している下記のセキュリティ事業のうち、貴社における利用状況に当てはまるもの		%
3. 普及啓発資料「組込みシステムのセキュリティへの取組みガイド」	1. 利用したことがある	33.3%
	2. 利用したことはない	33.3%
	3. 知らない	29.2%
4. 報告書「10大脅威 あぶりだされる組織の弱点！」	1. 利用したことがある	29.2%
	2. 利用したことはない	33.3%
	3. 知らない	37.5%



グラフ2.11　組込みシステムのセキュリティへの取組みガイド

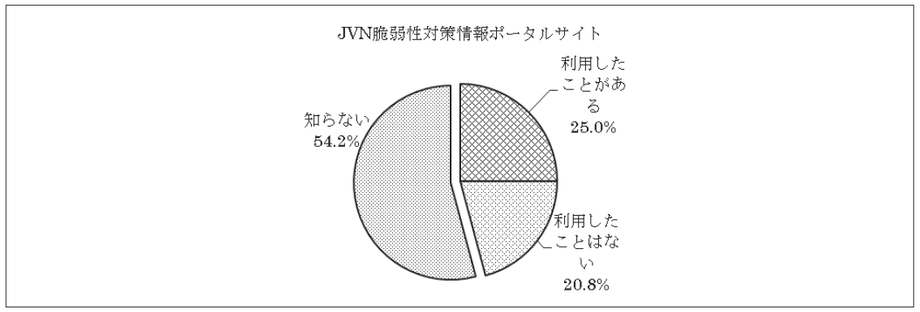


グラフ2.12　10大脅威 あぶりだされる組織の弱点！

2.7.4　IPAが実施している「JVN脆弱性対策情報ポータルサイト」について、貴社における利用状況は

表2.10

IPAが実施している下記のセキュリティ事業のうち、貴社における利用状況に当てはまるもの		%
5. JVN脆弱性対策情報ポータルサイト	1. 利用したことがある	25.0%
	2. 利用したことはない	20.8%
	3. 知らない	54.2%



グラフ2.13　JVN脆弱性対策情報ポータルサイト

第3章
GNU/Linuxシステムのセキュリティ

3.1　はじめに

本章では、GNU/Linuxシステムのセキュリティについて解説する。昔の組込みシステムは、単独で利用される機器ばかりだったが、現在では、外部メディアやインターネット接続が当たり前になり、テレビ、ビデオレコーダー、デジタルスチルカメラ、オーディオコンポ、携帯型オーディオプレーヤー、携帯電話などが有線LANや無線LAN等のネットワークに接続する時代になった。(**図3.1**　昔の組込みシステムと現在の組込みシステムを参照）そして、組込みシステムにGNU/Linuxシステムが採用される理由の一つとして、標準でネットワークに対応していることがあげられる。しかし、これらの組込みシステムはインターネットに接続された瞬間から、ネットワーク攻撃の脅威にさらされることになる。ここでは、Linuxカーネルやデバイスドライバそしてアプリケーションプログラムにはどんな脅威があるのか?そして、それらの対処方法と今後の対策について例を上げて解説する。

図3.1　昔の組込みシステムと現在の組込みシステム

3.2　組込みシステムに対する脅威

デジタル家電のセキュリティが注目された例としては、2004年の秋に、東芝製のHDD&DVDビデオレコーダー（RD-XS40など10機種）がブログへのコメントスパム攻撃に利用された問題（**図3.2**　株式会社東芝からのお知らせページ（http://www3.toshiba.co.jp/hdd-dvd/support/info/security/security.html）を参照）
が有名だろう。

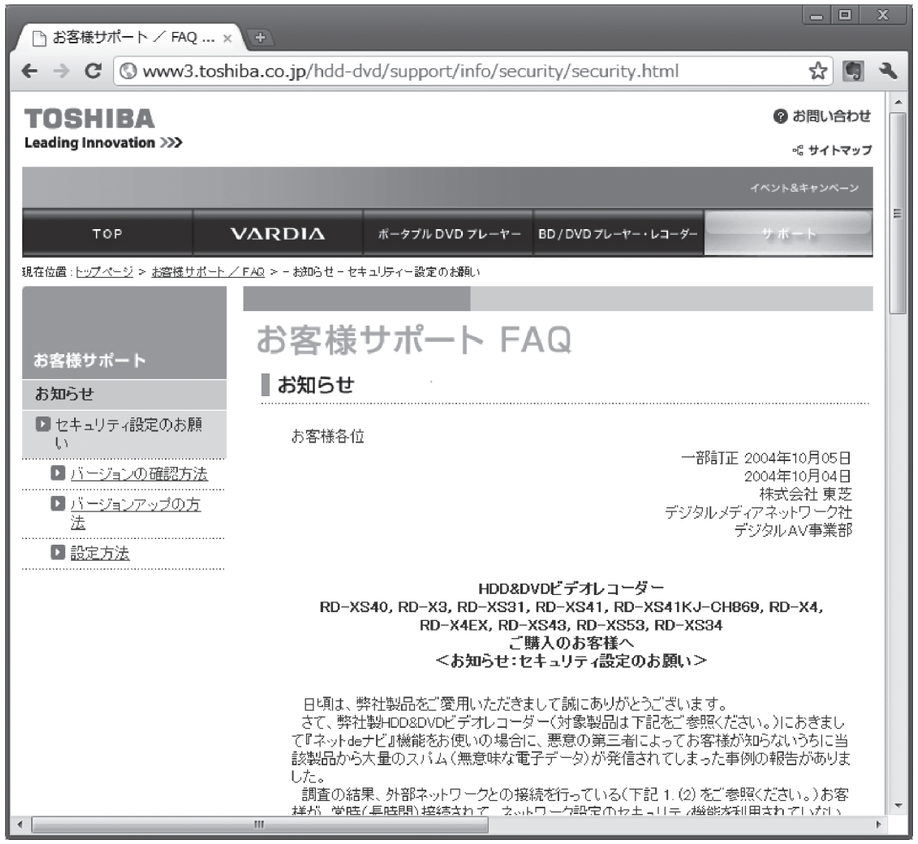


図3.2　株式会社東芝からのお知らせページ
（http://www3.toshiba.co.jp/hdd-dvd/support/info/security/security.html）

第6項　セキュリティ機能の有効化

Linuxのセキュリティ機能を使用するためには、カーネルのコンフィギュレーション時に、make menuconfigというコマンドを使用して設定する必要がある。（**図3.12**　make menuconfigを使用したセキュリティ機能の設定画面の例）

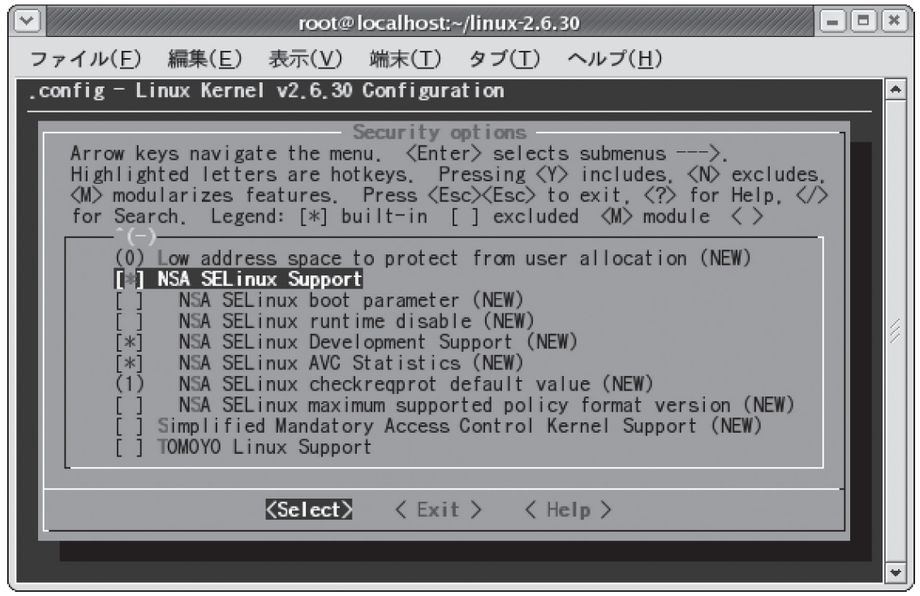


図3.12　make menuconfigを使用したセキュリティ機能の設定画面の例

なお、これらの機能は主にPC向けの機能として開発されたため、ext2/ext3/ext4ファイルシステム等のHDD用のファイルシステムの機能に依存している場合がある。よって、ファイルシステムの種類によっては使用できないものもある。例えば、組込みシステムでは、突然の電源断などにも対応できるようにJFFS2やYAFFS2等のジャーナリングファイルシステムが使用されることが多いが、これらのファイルシステムはext3ファイルシステムと同様の機能を持たないため、ext2/ext3/ext4等に依存する機能が使用できないという問題もある。現在では、それらの問題を解決するためのパッチが積極的に開発されている。

以上のように製品の仕様や使われ方に適したセキュリティ機能を選択する必要があるため、くれぐれもセキュリティ対策を怠ることのないようにお願いしたい。

なお、国際標準として、ISO/IEC15408 情報技術セキュリティ評価基準が存在する。ISO/IEC15408に基づきセキュリティ機能が正確に実装され、有効に動作することが評価できる仕組みも用意されているので興味のある方は調べてみるのも良いだろう。

3.3　脆弱性が発見されたときのプロセス

会員の皆様にもっとセキュリティに興味を持っていただくためにも、本節では脆弱性が発見されたときのプロセスについて説明する。

例えば、米国ではアメリカ国土安全保障省（U.S.Department of Homeland Security:通称DHS）のDHS National Cyber Security Divisionの運営部門であるUS-CERT(Computer Emergency Readiness Team)が、セキュリティ上の問題を監視している。もし、脆弱性を発見した場合は、cert@cert.org または soc@us-cert.gov 宛に報告するように求めており、発見された脆弱性はUS-CERT Vulnerability Notes Databaseで公開される。（**図3.4** 米国の脆弱性情報に関する組織を参照）

また、商務省(Commerce Department)配下の機関として国立標準技術研究所(National Institute of Standard and Technology:NIST)が存在する。そして、Computer Security DivisionのComputer Security Resource Center(http://csrc.nist.gov/)により全米脆弱性データベース(National Vulnerability Database)(http://nvd.nist.gov/)が提供されている。

さらに、US-CERTは、共通脆弱性と露出(Common Vulnerabilities and Exposures:CVE)情報を提供している非営利団体の米MITRE社を支援している。CVEは米MITRE社の商標であり、このCVEが事実上の標準となっている。また、脆弱性の対策が行われているかを手作業で判断するのには時間がかかるため、コンピュータのセキュリティ設定状況を自動で検査できるようにするための仕様として、XMLベースのセキュリティ検査言語OVAL(Open Vulnerability Assessment Language)が開発されている。

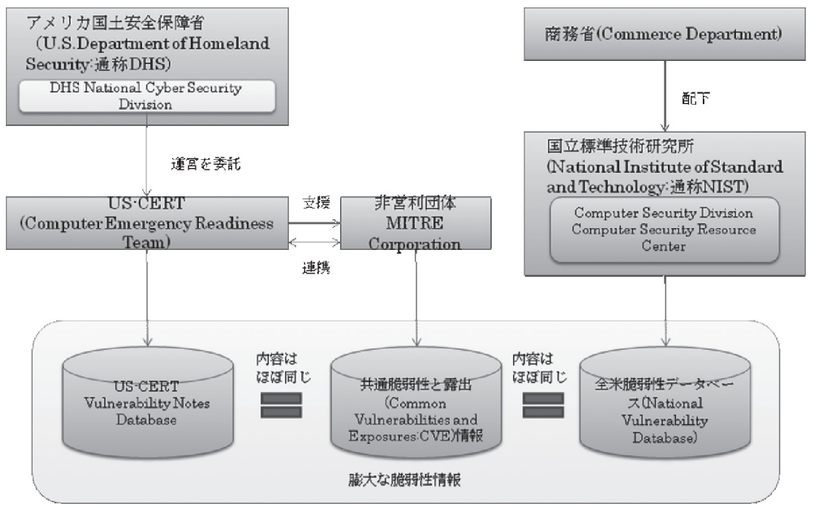


図3.4　米国の脆弱性情報に関する組織

表3.1　米国の脆弱性に関するデータベース

省庁	機関・団体	データベース
アメリカ国土安全保障省	US-CERT	Vulnerability Notes Database
商務省	NIST	National Vulnerability Database(NVD)
非営利団体	MITRE	Common Vulnerabilities and Exposures(CVE)

一方、日本では、US-CERTに対応するJPCERTコーディネーションセンターと呼ばれる組織が存在し、セキュリティ情報に関する注意喚起を行っている。(**図3.5**　JPCERTコーディネーションセンターのホームページを参照)

図3.5　JPCERTコーディネーションセンターのホームページ

また、独立行政法人情報処理推進機構(IPA)もJVN iPediaと呼ばれる脆弱性対策情報データベース(http://jvndb.jvn.jp/)を提供している。(**図3.6**　JVN iPedia 脆弱性対策情報データベースのホームページを参照)

図3.6　JVN iPedia 脆弱性対策情報データベースのホームページ

なお、IPAが発行する「組込みシステムのセキュリティガイドへの取組みガイド」では次のように報告されている。「組込みソフトウエアパッケージを利用する場合、販売元の脆弱性対策に関するサポート体制について事前に確認を行う。」「独自の開発プラットフォームを構成する場合、脆弱性対策情報を自ら収集する必要がある。その対策についても自主的に実施しなければならない。」つまり、組込みGNU/Linuxシステムの場合は、製品ごとにカスタマイズしたプラットフォームを採用するため販売元というものは存在しない。よって、脆弱性対策情報を自ら収集し、その対策を自ら実施する必要がある。

3.4　被害を最小限に抑えるために

GNU/Linuxシステムに脆弱性が全くないことを証明するのは難しいが、脆弱性が発見された場合の被害を最小限に抑えることは可能である。サーバーやクライアント用途に使用されるGNU/Linuxシステムで採用されている具体的な対策について説明する。

Linuxカーネルの開発では今まで様々なセキュリティ対応が行われてきた。2010年11月15日現在、最新のバージョンである2.6.36のLinuxカーネルではLSM(Linux Security Module)という共通の仕組みが用意されており、

- SELinux(Security-Enhanced Linux)、
- SMACK (Simplified Mandatory Access Control Kernel)、
- TOMOYO Linux、
- AppArmor (Application Armor)

という４つのセキュリティ拡張機能が取り込まれている。

また、これらの他にも、LIDS (Linux Intrusion Detection System) などの機能がコミュニティで開発されている。(**表3.2**　Linuxのセキュリティ機能を参照)

表 3.2　Linuxのセキュリティ機能

セキュリティ機能	ホームページ	提供形態
SELinux (Security-Enhanced Linux)	http://www.nsa.gov/research/selinux/ 開発元：米国家安全保障局 (National Security Agency：通称 NSA)	カーネルに取り込み済み
SMACK (Simplified Mandatory Access Control Kernel)	http://www.schaufler-ca.com/ 開発元：Casey Schaufler 氏	カーネルに取り込み済み
TOMOYO Linux	http://tomoyo.sourceforge.jp/ 開発元：株式会社 NTT データ	カーネルに取り込み済み
AppArmor (Application Armor)	http://en.opensuse.org/SDB:AppArmor 開発元：米 Novell 社	カーネルに取り込み済み
LIDS (Linux Intrusion Detection System)	http://www.lids.org/ 開発元：Kazuki Omo 氏	パッチでの提供

第1項　SELinux

SELinuxは、アメリカ合衆国国防総省 (United States Department of Defense：通称DoD) の諜報機関である国家安全保障局 (National Security Agency：通称NSA) が中心となって開発された。(**図3.7**　NSAのSecurity-Enhanced Linuxのホームページを参照)

図3.7　NSAのSecurity-Enhanced Linuxのホームページ

SELinuxでは、識別子 (identifier) としてラベルを用いてファイル等に対するアクセス権等の管理を行う仕組みを採用している。これにより、万が一、システムに不正に侵入された場合でも、侵入者はファイル等へのアクセスを禁止されるためほとんど何も出来ず、被害を最小限に抑えることが可能になる。

第2項　SMACK

SMACKは、Casey Schaufler氏らにより開発された。（**図3.8** SMACKのホームページを参照）SELinuxと同様にラベルを用いているが、複雑なアクセス権などをルールファイルで簡単に設定できる点がSELinuxと異なっている。例えば、AというプロセスからBというファイルへのアクセス権を簡単に設定することができる。

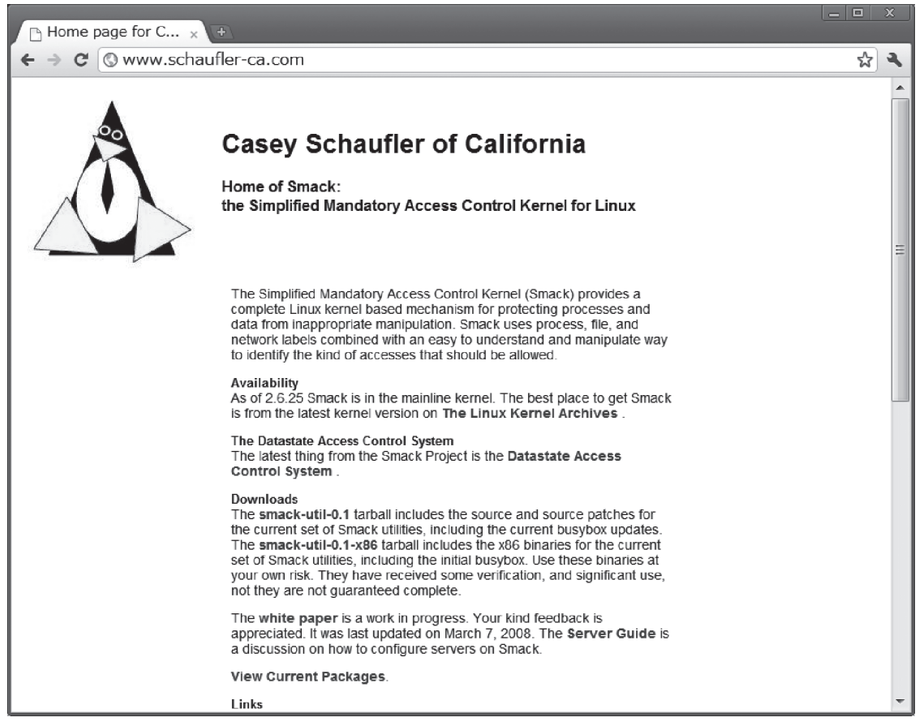


図3.8　SMACKのホームページ

第3項　TOMOYO Linux

TOMOYO Linuxは、（株）NTTデータにより開発された。（**図3.9**TOMOYO Linuxのホームページを参照）ファイルへのアクセス権や操作等を規定する「ポリシー」の自動学習機能を備えた強制アクセス制御（Mandatory Access Control）が特徴である。

図3.9　TOMOYO Linuxのホームページ

第4項　AppArmor

AppArmorは、SELinuxの置き換えを目的としてNovell社により開発された。（**図3.10** AppArmorのホームページを参照）よって、Novell社が開発しているSUSE Linuxのディストリビューションに標準で含まれている。

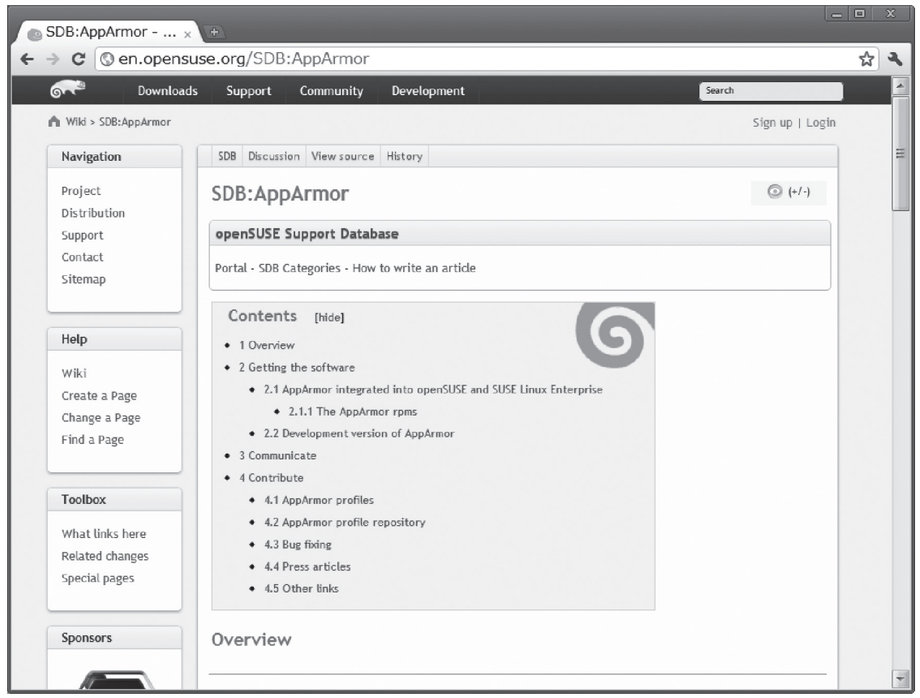


図3.10　AppArmorのホームページ

第5項　LIDS

LIDSは、Kazuki Omo氏により開発された。（**図3.11** LIDSのホームページを参照）2010年11月現在、2.6.32用のパッチが最新である。

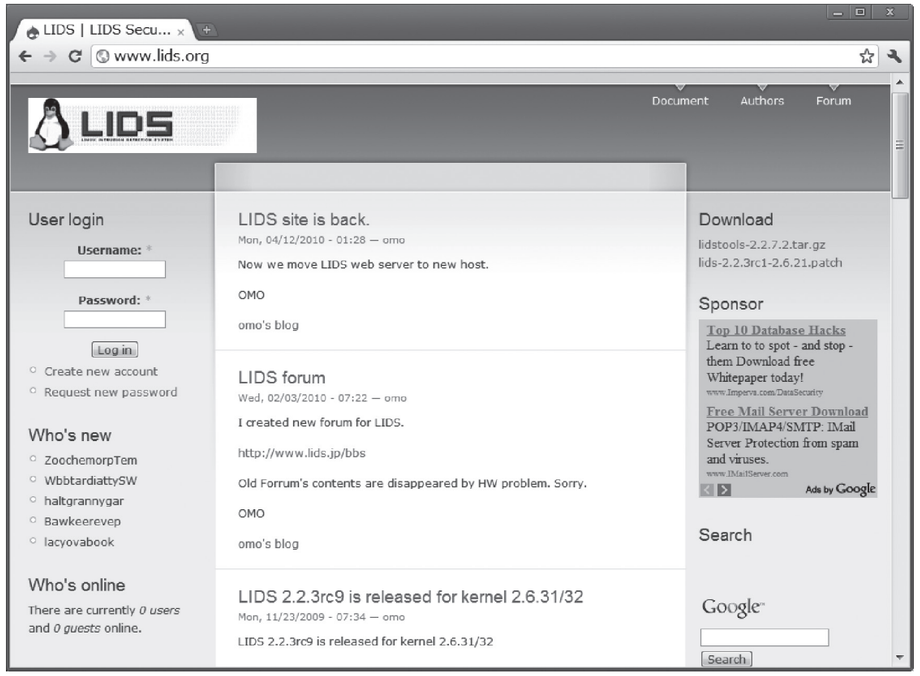


図3.11　LIDSのホームページ

第6項　セキュリティ機能の有効化

Linuxのセキュリティ機能を使用するためには、カーネルのコンフィギュレーション時に、make menuconfigというコマンドを使用して設定する必要がある。（**図3.12**　make menuconfigを使用したセキュリティ機能の設定画面の例を参照）

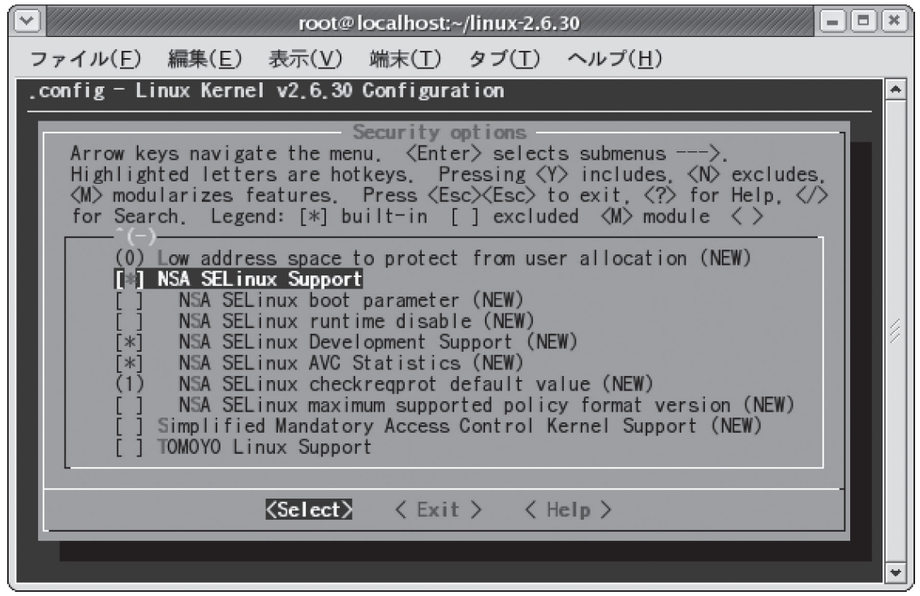


図3.12　make menuconfigを使用したセキュリティ機能の設定画面の例

なお、これらの機能は主にPC向けの機能として開発されたため、ext2/ext3/ext4ファイルシステム等のHDD用のファイルシステムの機能に依存している場合がある。よって、ファイルシステムの種類によっては使用できないものもある。例えば、組込みシステムでは、突然の電源断などにも対応できるようにJFFS2やYAFFS2等のジャーナリングファイルシステムが使用されることが多いが、これらのファイルシステムはext3ファイルシステムと同様の機能を持たないため、ext2/ext3/ext4等に依存する機能が使用できないという問題もある。現在では、それらの問題を解決するためのパッチが積極的に開発されている。

以上のように製品の仕様や使われ方に適したセキュリティ機能を選択する必要があるため、くれぐれもセキュリティ対策を怠ることのないようにお願いしたい。

なお、国際標準として、ISO/IEC15408 情報技術セキュリティ評価基準が存在する。ISO/IEC15408に基づきセキュリティ機能が正確に実装され、有効に動作することが評価できる仕組みも用意されているので興味のある方は調べてみるのも良いだろう。

第4章
組込みセキュリティと仮想化

4.1　仮想化技術とは

仮想化技術の要点は、絶縁である。エンタープライズ分野において、すでに仮想化技術が多用されているのは、まったく異なる顧客を、同一ハードウェアに収容しても、互いに絶縁されており、情報漏洩の心配が無いからである。

日本では、「仮想化」という言葉に曖昧さがつきまとっているが、アメリカでは、仮想化の分類が定着している。［参考URL　4.1］

仮想化技術は大きく分けて、

・プロセス・バーチャル・マシン

・システム・バーチャル・マシン

に分類される。

この2者は、まったく異なる技術であり、実現も目標も違う。

プロセス・バーチャル・マシンは、JavaVMなどであり。すでに1990年代末期より携帯電話などに採用され、その安全性は広く理解されている。

最近、エンタープライズ方面で採用が進み、組込みでも重要になってくるのは、システム・バーチャル・マシンであろう。

4.1.1　プロセス・バーチャル・マシン

プロセス・バーチャル・マシンは、JavaVMやUCSD Pascalで採用された「P-Codeマシン」、Smalltalk VM などが有名である。これらは、いわゆるインタープリタであり、UNIXやWindowsの一プロセスとして動作する。プロセス・バーチャル・マシンは、通常のアプリケーションの一つであり、OS機能や計算機資源へのアクセスも通常のOS APIを使用する。よって、実行権限、システムへ与える危険性は、一般のアプリケーションとまったく同等である。

インタープリタは、その上で実行する対象の、メモリのアクセスを制限することが一般的であり、実行時に動的にメモリ・アクセスの範囲が適正か否かを判断して、安全なメモリ・アクセスだけを実行する。よって、一般的にインタープリタによる実行は、セキュリティ脆弱の無い、安全な実行であることが普通である。

ただし、Java実行系(JavaVM)をはじめとする最近のインタープリタ(Ruby VM,

JavaScriptインタープリタなど)は、JIT(Just in-Time compiler) [参考URL 4.2]という機構で、動的に機械語のコード列を生成し、その生成されたコードを実行することが多い。JIT機構が入った実行系は複雑度が高く、検証を十分に行わないと、セキュリティ脆弱性が皆無であるかどうかは、安易には判断ができないだろう。

UNIX/Linuxなど、計算機資源へのアクセス権限が適切に設定できるOS上で動作している、プロセス・バーチャル・マシンは比較的安全である。そのプロセスに過大な権限を与えなければ、仮に仮想マシン・インタープリタにセキュリティ脆弱性や、メモリを壊す欠陥があったとしても、被害は、そのプロセスのユーザ(OS管理上のユーザ)の範囲に留まる。

μiTRONなどの旧来のメモリ保護の無いRTOSやOS無し環境の場合には、プロセス・バーチャル・マシンの脆弱性が、システム全体に影響を及ぼす恐れがある。携帯電話でJavaが採用されたのは、仮想マシン・インタープリタによる安全性が主要な要因である。Java導入時、多くの携帯電話はメモリ保護の無い、μiTRONクラスのOSを使用していた。インタープリタの信頼性が高ければ、外部からプログラムをダウンロードして実行しても、セキュリティ脆弱性が発生する心配は無い。

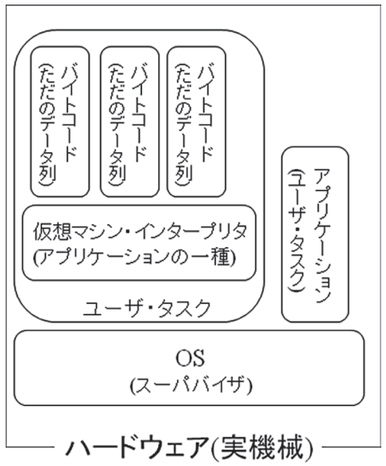


図4.1 プロセス・バーチャル・マシン

4.1.2 システム・バーチャル・マシン

システム・バーチャル・マシンは、仮想機械モニタ(バーチャル・マシン・モニタ,以下 VMM と表記)やハイパバイザ(Hypervisor)と呼ばれるソフトウェアが、常駐し、一台のハードウェア上で、あたかも複数のハードウェアがあるように見せかける。

システム・バーチャル・マシンの仮想化でいう「絶縁」とは、メモリの参照(書き換えを含む)ができないということである。

独立した仮想機械同士は、他の機械からメモリを決して読みとられたり、書き込まれたりしない。

UNIX/Linuxのプロセスも本来はそういう関係にあるが、UNIX/Linuxでは管理者の設定ミスなどにより、特定のプロセスに強大な権限を与えうる。そして、そのプロセスは他のプロセスのメモリやファイルを読み書きしたり、所有権を書き換えたり、あらゆることを行うことができる。

それに対して、仮想機械の間では、そのようなことは起こり得ない。仮想機械間の通信は、実メモリを共有するとしても、制限された特定に領域だけの、共有が行われる。ある仮想機械内で、特権を得たものがあったとしても、それは仮想機械を越えて、自仮想機械以外のメモリを読み出したり、書き込んだりすることは、絶対にできない。

各仮想機械では、個別にまったく異なるOSを動かしたり、OS無しアプリケーションを動作させることができる。

VMMは各仮想機械が干渉しないようにしながら、計算機時間を適切に各仮想機械に割り当てる。

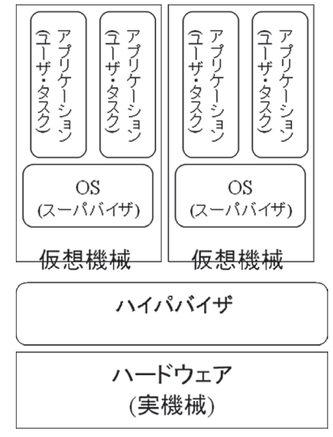


図4.2 システム・バーチャル・マシン

システム・バーチャル・マシンの絶縁のもっとも重要な技術は仮想メモリ管理である。仮想メモリ空間の設定管理と実メモリの管理をVMMが正しく行うことに よって、絶縁を実現する。ここでいう絶縁とは、実メモリが決して共有されず、ある仮想機械のメモリを、他の仮想機械からは決して読み書きできないということである。それによって、情報の漏洩や、干渉がなく、セキュリティが絶対的に守られる。

ディスクに関しては、パーティションを切ってしまい、VMMは、ある仮想機械が他の仮想機械のパーティションには絶対にアクセスできないようにする。

実ハードウェアに仮想記憶機構がある場合、VMMはそれを利用して、絶縁を実現する。VMMは、仮想機械からは特権のある制御が一切できないようにする。仮想機械上のOS(「ゲストOS」と呼ばれる)が、仮想記憶管理ハードウェア等にアクセスするとき、特権がないので、アクセス違反が起こり、制御がVMMに移る。VMMは、ゲストOS の意図とパラメータを読み取り、適切に嘘の実アドレス操作を行う。 それによって、ゲストOSとその仮想機械は、あたかも自由にハードウェアを操作していると思いこまされるが、実際には、VMMが管理するメモリ空間と実メモリで、騙されて動作している。

大型計算機(いわゆる汎用機)では、システム・バーチャル・マシンは、IBMSystem360上で、1966年から実現されている。汎用機では、外部IOとのやりとり は、すべてIOチャンネルにDMAで行わせていた。IOチャンネルにDMAアドレスを指示する時も、VMMが介入し、適切にDMAアドレスを調整する。それによって、汎用機では、OSやアプリケーションなどの変更無しに、仮想機械化を行うことができた。

元来のVMMは、一般に、単純であり、実メモリ、仮想メモリ機構、CPU時間割り当て、ディスクのパーティションを管理する。単純なVMMは、信頼性を確保するのが容易である。

IBMは、1966年当時、マルチユーザ、マルチタスク、仮想記憶管理の全てを備えたOS(現在の通常のTSSシステム)を作るよりは、VMMを開発し、VMM管理下で複数の仮想機械を起動し、その中で、シングルユーザOSやシングルタスクOSを、動作させる方が容易であると判断し、System 360を仮想化した。

現在、データセンタなどのエンタープライズ分野では、x86 CPU上で、Linuxを中心に仮想化を行ったシステムが実用的に多数運用されている。

一般のデータセンタでは、外部ネットワークの接続が律速(速度のボトルネック)になっており、高速なCPUの能力には十分に余裕がある。その装置に、十分な絶縁のもとで、複数の顧客を収容することは、コスト・パフォーマンスの向上、電力と設置面積の節約になり、急速に広がっている。

ただし、x86 Linuxでは、マイコンや低クラスのミニコンのOSが一般的に行っているように、IOポートを直接にメインのマイクロ・プロセッサが操作していた。特に、x86のIOポートは、IO空間という特殊な空間にあり、メモリ管理ユニッ トの操作では、まったく管理できない。そのため、x86での仮想化の初期は、そのままでは仮想化がうまく実施できなかった。とくに、ビデオ・ディスプレイに各ゲストOSが アクセスするという競合が問題になった。しかし、現在の x86 Linuxは、IOデバイスドライバ・ソフトウェアのほとんどが仮想化対応になり、ネットワーク、ビデオ・ディスプレイをはじめとするほとんどの装置に問題がなくなった。

そもそも仮想化を行うシステムは、TVゲームを実行するような用途ではないので、ビデオ・ディスプレイのハードウェアに高速に直接アクセスする必要はない。

VMMにセキュリティ脆弱性や決定的な欠陥が無ければ、仮にある仮想機械上のゲストOSである Linuxにセキュリティ脆弱があったとしても、それが他の仮想機械に影響を及ぼす恐れはない。一つのハードウェアに多数の顧客を収納しても、各顧客ごとに、仮想化して絶縁しておけば、ある顧客のLinuxがセキュリティ侵害されても、その影響や被害が、他の顧客の仮想機械に及ぶことはない。

エンタープライズ分野では、システム・バーチャル・マシンによって仮想化されたシステムが、すでに多数運用されている。データセンタのコスト・パフォーマンスの向上のために、より一層の、システム・バーチャル・マシンによる仮想化が急激に進んでいるところである。例えば、ある業務領域では、「クラウド・コンピューティング」と言えば「仮想化技術の導入」と考えられているほどである。しかし、仮想化とクラウド・コンピューティングは直接には関係ないのであるが。

4.2 組込み分野での仮想化の要請

組込み分野でも仮想化の要請は存在する。

Javaに代表されるプロセス・バーチャル・マシンは、すでに携帯電話などで使用されて、10年以上の実績がある。

ここでは、システム・バーチャル・マシンについて述べる。

現在、組込み分野でも、IOの遅さに比べて、CPUコアは十二分に速い。そこで一つの物理CPUコアに、複数の仕事を行わせたい。しかし、これまですでに検証されたソフトウェア・システムは、OSを含めて変更したくは無い。そこで、仮想化を行い、仮想機械ごとに、ソフトウェア・システムの一式を丸ごと載せる。各システムは完全に絶縁され、干渉しない。そうすれば、ソフトウェアの組み合わせによる不安と検証工数は大幅に減少できる。

また仮想機械方式であれば、RTOS(実時間OS)と、Linuxなどのいわゆる IT情報系OSを同一ハードウェアに収容でき、Linuxにすべて載せ替えて実時間性の実現に苦悩するということもない。(ただし、実時間性を保証するVMMを採用しなければならないが)

Linuxは複雑度が高い。またシステム外部のネットワーク、とくにインターネットに接続することが多い。RTOSとLinuxを一緒に収容し、動作させていた場合に、Linuxがセキュリティ脆弱性を突かれたとしても、仮想化技術で絶縁されていれば、Linuxの影響がRTOSに及ぶことはない。

また逆に、RTOS使用のシステムが、メモリ・アクセスのバグで、RTOSを引き連れてシステム全体がフォールト状態に陥ってしまっても、それはその仮想機械に閉じており、Linuxや他のRTOSを動作させている仮想機械には影響が及ばない。必要があれば、他の仮想機械上のゲストOSのアプリケーションから、他の仮想機械の健康状態を監視させ、フォールトが発生した仮想機械をリセットさせ、そのシステムを再起動させることも可能である。監視を行うにあたっては、監視する側と、監視される側がアクセスするデバイスを

作成したり、定期的に仮想機械間で通信を行うような、システム設計をしておく。(元来、仮想機械どうしは絶縁されているので、他の機械の健康状態を覗き見るようなことは実現できない。もし、仮にそういう便利な機構を用意すると、それを利用したセキュリティ破りが発生することが常である)

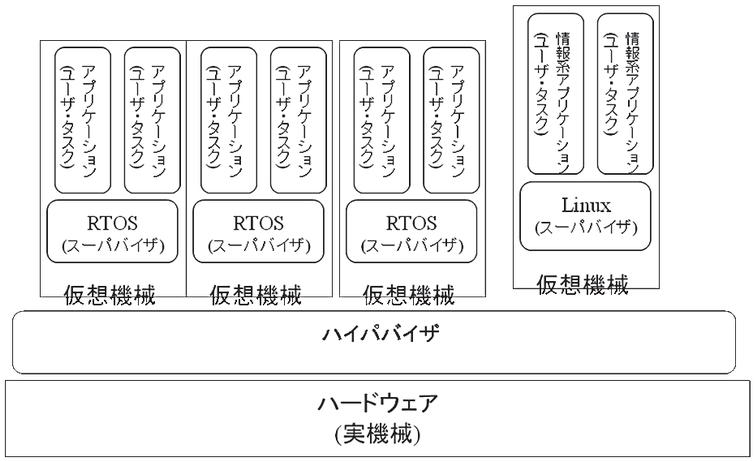


図4.3　RTOSとLinuxを同一ハードウェアに収容

組込み分野では、同種のOS(特にLinux)を、バージョンを変えて複数同時に動作させたいという要請もある。その場合も、仮想化技術で、複数の仮想機械で個別に Linuxを動作させれば、複数の版のLinuxを同時にいくつも起動できる。

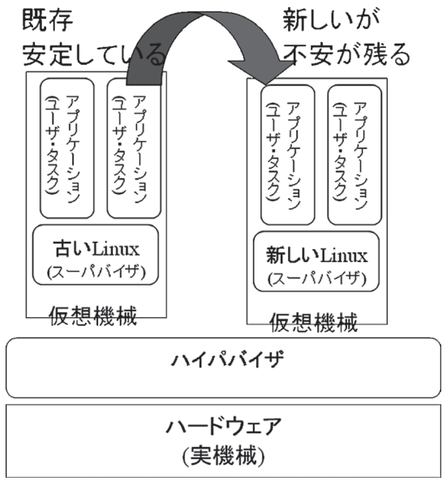


図4.4　バージョンの異なるLinuxを同一ハードウェアに収容

組込み分野は、ソフトウェアのライセンス問題も抱えている。エンタープライズ分野では、オープンソース・ソフトウェアを、そのライセンスに従って運用しても、守秘義務や、市場での競争に、ほとんど影響がない。

組込み分野で、オープンソース・ソフトウェアをそのライセンスを理解せずに迂闊に採用してしまった場合、機密度の高いハードウェア・デバイスの情報や、市場競争上重要なソフトウェア機能を公開したり、無料で使用権を許諾したりしなければならなくなる。

そういう問題から、はっきりと逃れるには、オープンソースの入ったソフトウェアはある仮想機械の中で動かし、私的財産のソフトウェアや機密度の高いデバイスを駆動するソフトウェアは別な仮想機械で動かすと良い。そうすればオープンソースのライセンスに私的財産は汚染されない。また、仮想機械の絶縁性は、世界的に広く一般に認知されているので、オープンソースのライセンスに私的財産が汚染された、と誤解される可能性も極めて低い。

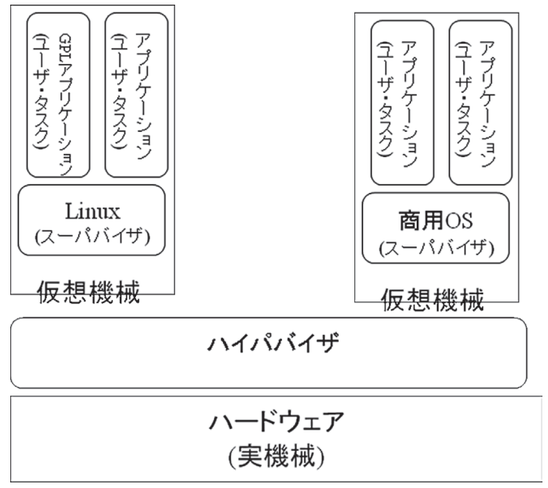


図4.5　GPLソフトウェアと私的財産の絶縁

4.3　組込み分野での仮想化技術

現在は、半導体メモリ・チップの1つの容量が大きくなり、IT系技術を使用するシステム(Blurayプレーヤ、北米版デジタルTVなど)では、組込みシステムでも、32M Bytes～64M Bytesのメモリを搭載する機器が普通になってきた。通常、これまでの組込みLinux使用のシステムは、アプリケーションのワーキング・エリアを入れても、32M Bytes程度で充分動作する。したがって、現在、異なるLinuxを2組同時に動作させる程度の実メモリは組込み機器に備わっている。また、Linuxを動作させるCPUはMMU(メモリ管理機構)を備えており、仮想化技術を実現するハードウェア機能は持っている。

システム・バーチャル・マシンのメモリ空間の絶縁技術そのものの原理は、単純かつ明解であり、メモリ空間分割(絶縁)を担当するソフトウェア・モジュールを作成するのは、さほど困難ではない。

また、仮想機械を時分割でスケジュールする方法は、原理的にはTSS(マルチユーザ・マルチタスクのタイムシェアリング・システム)と同じ考え方であり、原理的な困難はない。ただし、ゲストOS下のアプリケーションの実時間性を保証したり、イベントに対する応答性能を向上させるための、標準的な方式は確立されていない。

多くの既存CPUや既存組込みCPUで、仮想化を行うことは、原理的には可能なのではあるが、仮想化を支援するハードウェア無しに、効率よくゲストOSや、アプリケーションを実行するのは、難しい場合がある。

以下では、代表的な組込みCPUについて考察する。

MIPSアーキテクチャは、ハードウェア支援が皆無であっても、純粋な仮想化(pure virtualization)も比較的効率低下が小さく実現できる。MIPSアーキテクチャでは、ゲストOSが使用する一部の特権命令を別な命令列に書きかえる準仮想化(para virtualization)を行うと、容易に比較的高い性能を得られる。

ARM6,7,11アーキテクチャは、純粋な仮想化は不可能である。ARMアーキテクチャでは、一部の重要なシステム・レジスタへのアクセスを、VMMが捕捉できず、仮想化を実現することができない。したがって、ゲストOSが使用する特権命令を別な命令列で置き換える準仮想化が必須である。

古いx86アーキテクチャでも、純粋な仮想化でシステムを動かすことも可能だが、新しいIntel CPUが備える「VTx」機構が、IO、特にDMAに関して仮想化対応を行ったので、非常に効率的に仮想化技術を実行することができる。組込みを主ターゲットにしているIntelのATOMシリーズは、VT機構を備えているものと、備えていないものがある。ATOM CPUの選定は、詳しく調べて行わなければならない。

4.4　組込み用仮想化技術とセキュリティ

プロセス・バーチャル・マシンであるJavaは、ソフトウェアによる、メモリ・アクセス、IOアクセスのチェックがあり、メモリ保護の無いOS下であっても、いかなるアプリケーション・プログラムも安全に実行できた。それに加えて、Java組込みエディション(MIDP),JavaSEなどではファイル・アクセスやネットワーク上のサーバのアクセスにも、制限が付いていた(特別に設定を行った場合だけ、それらのアクセス制限を外せる)。それらの制限により、セキュリティに特に注意を払わない人々が作成したシステムでも、安全に運用できた。

Javaが携帯電話に10年間以上の間採用され続け、極めて多数の端末が運用されているにも関わらず、セキュリティ事故が発生していないのは、プロセス・バーチャル・マシンの安全性が示されていると考えて良いだろう。ただし、JIT機構が入ったJavaVMは、先に述べたように、複雑度が高いので、よく検証されたもののみを採用すべきである。JIT機構の生成するコードは、ガベージコレクション(ゴミ集め)回りに問題が出やすく、それがセキュリティホールにつながらないとは限らない。

システム・バーチャル・マシンによる仮想化技術は、エンタープライズ分野のデータセンタで、すでに多数が運用されている。これまで、とくに、絶縁性(ひいてはセキュリティ)に関わる事故は起きていない。

メモリ空間の絶縁技術そのものの原理は、単純明解であり、メモリ空間分割(絶縁)を担当するソフトウェア・モジュールをセキュリティ脆弱性無しに作成するのは、さほど困難ではない。システム・バーチャル・マシンは、1966年にIBMがSystem360上に仮想化システムを実現した時と、原理は変わっておらず、根本的には、セキュリティ脆弱性は発生しにくい。

システム・バーチャル・マシンを採用し、複数のシステムを一つのハードウェアに収容すれば、あるゲストOS(例えばLinux)がセキュリティ脆弱性を突かれて、その特権を取られても、他のRTOSやLinuxのメモリは読み取られることが無い。よって、いわゆるIT系の複雑なOSを、高セキュアであるべき組込みシステムに組み込んでも、セキュリティに関する脅威は増加しない。

システム・バーチャル・マシンでは、仮想機械間通信を利用して、ある仮想機械を別な仮想機械で監視させることが可能である。こういうバイタル・チェック(健康チェック)、ハートビート・チェックなどにより、仮想マシン内のシステム(ゲストOS)がフォールトを起こしたことや、その振る舞いによってはセキュリティを破られたことを、検知することができる。

このように、システム・バーチャル・マシンは、組込みシステムの高信頼化と高セキュア化に貢献する。ハードウェア資源に余裕ができ、電池駆動や省電力を進めるべき現在、仮想化技術による、複数ソフトウェア・システムの収容は組込み分野でも役立つであろう。

■参考URL4.1

仮想機械（英語版WikiPedia）

http://en.wikipedia.org/wiki/Virtual_machine

■参考URL4.2

JIT（英語版WikiPedia）

http://en.wikipedia.org/wiki/Just-in-time_compilation

第5章
クラウド時代のセキュリティ

5.1　はじめに

クラウドは、いまビジネスでの利用が取り沙汰されるが、むしろリソースを持っていない個々の市民の利用が今後増加してくると思われる。極端に言えば無限のリソースを消費者個人が獲得する時代がくるかも知れない。現在の統制なきネットワーク利用のまま、そうなった世界はどうなるだろうか？情報へのアクセスに制限を設けるべきではないかも知れない。しかし、ITは単に情報伝達するだけのツールではない。もともと制御系のツールとしての歴史は長いし、家電ホームエレクトロニクスの制御が、ネットワークを通じて広範囲に行われることになるだろう。モラルの確立する前の子供が何ら制御なくクラウドにより無限のリソースを使って家庭の制御系をハッキングしコントロールする時にどんなリスクが発生するか、想像するのさえ怖いものがある。従って、自らのコントロール権の喪失からくるリスクの存在があるからこそクラウド時代の今IT統制が求められるようになってきている。

5.2　IPv6やNGNの普及

今普及しているIPv4は2011年5月にも枯渇すると言われている。NGN（Next Generation Network）もIPv6を利用した閉域網であり、インターネットとの相互接続に問題が出ている。しかし、IPv6の普及によって128ビット（340澗、１澗は１兆の１兆倍の１兆倍）ものアドレスから生み出される。このようなネットワーク環境では、**図5.1**に示すように各家電製品をはじめスマート・メータと呼ばれる装置などもネットワークに接続されるようになり、個人情報を含む情報全般の保護は必須の機能となりつつある。

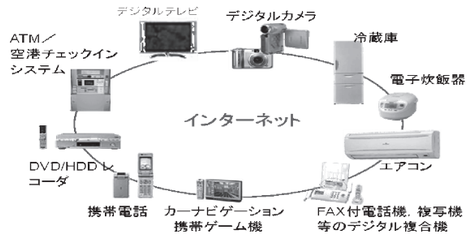


図5.1　何でもつながる時代の到来

ましてやIPv6は安全対策が現時点で十分ではない。IPv6のアドレス数は無限大に近いので、全ての機器にインターネット上のグローバル・アドレスを割り当てられる。従って、インターネットから全ての機器を直接呼び出せるので、インターネット・ユーザーが不正アクセスの不安に直面することになる。

これに対してIPv4はインターネットでは、殆んどの場合組織内でのみ通用するIPアドレス(ローカルアドレス)をマスカレード[4] (NAPT:IP masquerade) などアドレス変換技術を使ってインターネット上のアドレス(グローバルアドレス)へ変換するので、他インターネット・ユーザーに自分のパソコンのIPアドレスを知られずに済む。つまり、IPv4の場合、悪意のある第三者に狙われる危険性は小さくなるが、IPv6の場合は例えば、悪意のあるグループがクラウドを使って、通信経路を操ることができることになる。

膨大な量のアドレスは、効率的な経路制御ができないとネットワークが破綻してしまうので、国際電話番号のようにグローバルには、国番号＋市外局番＋電話番号のように階層化することでこの問題に対処するようになるであろう。

また、一般家庭環境のように、モバイルやクラウド・コンピューティングが普及し、ファイアウォールやプロキシに守られない環境が一般化するときには、セキュリティは特に重要な機能となる。

一方では、IPv6では、標準でセキュリティに関する機能が用意される。具体的には、IPv6は端末間の通信をIPSecで守ることが必須であり、認証や暗号化に対しても、認証ヘッダ (Authentication Header : AH) と暗号化ヘッダ (Encapsulated Security Payload : ESP) が、それぞれ拡張ヘッダとして組み込まれている標準プロトコルでもある。しかし、所属セグメントが動的に変わるMobile IPが可能となる仕組みも提供しているが、これは移動端末ゆえの脆弱性となる。

いずれにせよ、コンピュータの性能は35年間で65万倍に、同じく光通信容量は3.5万倍と大きく進歩する一方、クラウドのスケールアウト機能により、ITの利用自体が無限に増殖し、それに伴ってリスクも増加する。これは従来の発展 (Development) ではなく、パラダイムシフトを伴った不連続な変貌 (Transfiguration) とも言える。すなわち、情報という新しい経済材がコンピュータとネットワークの機能拡大によって安いコストの交換が可能となり、更にクラウドによって処理が無限にスケールアウトの可能性を持ったことになる。

さらに、〇〇制御系と称される機器内部に組み込まれたコンピュータシステムは、計測用・制御用ソフト、FA (ファクトリオートメーション) 用ソフト、組込み用ソフトなど

4 インターネット上で、一つのグローバルなIPアドレスを複数のコンピュータで共有する技術。ローカルアドレスと、グローバルアドレスを相互変換することにより実現される。NAT(Network) Address Translation) と異なりTCP/UDPのポート番号まで動的に変換されるため、一つのグローバルアドレスで複数のマシンから同時に接続することが可能である。ただし、ポート番号の変換が行なわれるため、制限がある。もともと「NAPT」が技術の名称で、「IPマスカレード」はLinuxにおけるNAPTの実装のことだったが、現在では両者が混同されている例が多く見られる。また、ブロードバンドルータのスペック表などではNAPTの意味で「NAT機能搭載」と表記していることもある。

範囲が急激に拡大する。しかもこれらはメーカ以外の一般利用者には眼に触れずファームウェアとして例えば電子ジャーやビデオ装置、自動車などの内部にBlack Boxとして装備される。これらの機器をクラウドからネットワークを通じて「制御する」となると、組込みシステムの場合には、直接的に人命にも係るリスクが生ずることが予想される。
特に、SCADA (Supervisory Control And Data Acquisition) の事例は、深刻になりがちである。SCADAとは、産業制御システムの一種であり、コンピュータによるシステム監視とプロセス制御を行う。対象プロセスは、生産工程やインフラや設備に関する重要インフラである。SCADAのセキュリティについては、従来から、サイバー戦やサイバーテロリズムの危惧から、指摘が出されて来ていたが、今回2010年7月のNY Times記事中で、明らかにSCADAをターゲットにしたエクスプロイットが登場したことで、現実の問題として認識するされるようになった。日本でもSCADAは各方面で使われているので、今後クラウド化に向けて将来に備えて警戒が必要な分野と言えると思われる。

5.3 内部統制とクラウドとの関係

クラウド時代には、組織に属する人々は勿論のこと、個人の資格でもクラウドを通じて膨大な量の資源を使えるようになる。例えば契約によっては、開発環境を手に入れることも可能である。そこで悪意を持つ組織がマルウェアを開発し、デジタル家電等を攻撃することも可能となるだろう。デジタル家電の開発者はセキュリティには詳しくなく、ゲーム機などモラルや悪意を持たない子供も含まれる。しかし情報はそのもので人間その他の身体的危害を加えることは不可能である。少なくとも一般的なIT環境はこれまで限界があって、それ自体が防御壁となって機能しているからだと言える。従って、クラウド側で何らかの統制をかけないことにはこのような攻撃を防ぐことはできない。

一方、内部統制のフレームワークは、米国トレッドウェイ委員会組織委員会 (COSO) が1992～1994年に公表した報告書「Internal Control - Integrated Framework (内部統制－統合的枠組み : 俗にCOSOレポートという)」で提唱されている。その中で、内部統制の定義は、「以下に分類される目的を達成するために、合理的な保証を提供することを意図した、取締役会、経営者およびそのほかの職員によって遂行される1つのプロセスである。その内容は、財務諸表に対するもので、①業務の有効性・効率性、②財務諸表の信頼性・関連法規の遵守」とされている。さらに、内部統制の構成要素として「統制環境」「リスクの評価」「統制活動」「情報と伝達」「監視活動」を5項目挙げ、これらを内部統制を評価する際の基準として位置付けている。日本では、証券取引法の抜本改正となる金融商品取引法 (日本版SOX法) が2006年6月に成立。2009年3月期の決算から、上場企業に内部統制報告書の提出・公認会計士によるチェックが義務付けられている。

クラウド・コンピューティングでは、データの完全性や機密性、すなわちベンダ企業

のデータに関する秘密保持責任がこれまであまり明確にされて来なかった。クラウド・コンピューティングの普及に伴い、この点が極めて重要な課題となってくると予想される。クラウド以前のデータセンタ利用の段階では、企業は個別の事業者と直接契約を行うか、あるいは間接契約の場合においてもシステムインテグレーター（SIer）を通じて自社の情報にアクセスを行う可能性のある事業者全体を把握することが可能であった。しかし、クラウド環境においてはクラウド事業者同士が連携して、より柔軟かつ堅牢な計算環境を構築することが予想される一方、どのクラウド事業者が顧客のデータを扱うことになるのか、正確に把握することが困難になると考えられる

また、SaaSでは、データベース中において顧客別のアクセス制御が行われない実装が現時点では多く見られるため、個々のアプリケーションレベルでのアクセス制御を実装するように変えていく必要があると考えられる。

クラウド・コンピューティングでは、データの完全性や機密性等のデータ保護策、すなわちベンダ企業のデータに関する秘密保持責任がこれまであまり明確にされてこなかった。一方、利用者のデータのセキュリティ等に関する事項について免責規定を置いていることも多い。IPv6やNGNの普及に伴い、クラウド・コンピューティングにおいては、極めて重要な課題となってくると予想される。

一方現時点では、SAS70等の外部監査報告書は、第三者の監査によりクラウド・コンピューティング・サービスにおけるセキュリティを含めた内部統制について唯一担保するものである。海外の一部のクラウド・コンピューティング・サービスでは、例えば、Salesforce.comは同社が提供するオンデマンドCRMサービスである“Salesforce.com”について2004年にSAS70（米国監査基準書70号）Type IIの監査を既に完了し、SysTrust[6]の監査も終えている。Googleにおいても、同社が提供するコミュニケーションやコラボレーションのためのツール類である“Google Apps”について2008年11月にSAS70 Type IIの監査が完了したことを発表した。このように、セキュリティが何らかの形で担保されない限りは、利用者は安心してクラウド・コンピューティングを利用することができない。日本においても、どのような方法でデータセンタのーセキュリティを確認、担保していくべきか、極めて重要な課題である。クラウド事業においてデータ管理の安全性を確保した上で、事業者選択を適切に行うためには、データ管理対策に関する統一された情報公開フォーマットの策定と、表明するデータ管理対策を第三者が監査・認証するための監査スキームの確立等を検討する必要があると考えられる。

5.4 個人認証の重要性

正当な権利を有する者が、必要な時に正しいサービスの提供を受けることを保証するためには、アクセスしている者が正当な権利を有する者であることを合理的な方法で検証できることが必要である。こうした検証の手段として認証技術がある。現在、主に用いられている認証技術としては、利便性の高いID・パスワード方式、セキュリティ強度の高いICカード等を用いたPKI方式などがある。最近では、生体情報を用いた方式も用いられてきている。

個人を認識するため、現在、民間においてOpenID[7]やリバティアライアンス[8]プロジェクト等、複数のウェブサイト間で、IDを連携するID管理の取組が進んできている。ID管理とは、ユーザーの識別・属性を複数のシステムにまたがって管理することで、このようなID管理をより一層促進してゆくためには、それぞれのウェブサイトで要求する認証に関する本人確認のレベルと認証技術の強度を、ある程度一定に統一しておくことが重要である。例えば、他の機関で行われた本人確認結果が共有可能となることによって、効果的な連携・運用の促進に寄与することができる。また、ID管理とデータ連携が重要になるケースが多いと思われる。

特にクラウド・コンピューティングの場合、課金と直接結び付くアカウント情報の管理が問題となる。クラウドを使う側は、通常ニーズに従って複数のサービスを使い分ける。その都度サービス毎に発生する認証のためID情報とパスワードの入力が必要となる。その度に漏洩のリスクも高まるので、アカウント情報の入力回数を減らす為に、「シングルサインオン」が重要となる。さらにこの認証サービスをクラウドのサービス提供業者か

5 SAS70 Type II：SASはStatement on Auditing Standardsの 略。AICPA(American Institute of Certified Public Accountants：米国公認会計士協会）の取り決めた監査基準で国際的に認められている。No.70は「サービス機関により行われている取引の処理に関する報告(Reports on the Processing of Transactions by Service Organizations)」(1992)。AICPA職業基準書のAUセクション423に対応。2002年のSOX法(Sarbanes-Oxley Act）セクション404では、サービス部門については正確な内部コントロールが必要であるとし、このSAS 70監査報告を必須としている。SASはStatement on Auditing Standards の略。No.70は「サービス機関により行われている取引の処理に関する報告(Reports on the Processing of Transactions by Service Organizations)」(1992)。AICPA職業基準書のAUセクション423に対応。SAS70のレポートには、Type ⅠとType Ⅱの2種類があり、Type Ⅰでは、アウトソーシングサービス事業者が、委託元企業の財務諸表監査に関係する自己の内部統制を記述し、独立監査人が、ある基準日において、内部統制が統制目標達成のために適切に設計され、整備されているかという点についての意見を表明する。Type Ⅱでは、Type Ⅰのレポートに加え、独立監査人が、所定の期間を通じて内部統制が有効に運用されていたかどうかの検証を行い、その有効性について意見を表明する。

6 企業の情報システムの内部統制について「SysTrust原則および規準」にもとづき特定の期間において有効に運用されているかを公認会計士が検証するサービス。SysTrustの保証規準としては、以下の4つの「SysTrust原則および規準」が設けられている。 ①可用性原則（Availability)、②セキュリティ原則（Security)、③インテグリティ原則（Integrity）④維持性原則（Maintainability)。もともとは米国公認会計士協会とカナダ勅許会計士協会により開発されたもので、
具体的には以下のような検証報告書が発行され、Webサイトで確認できるようになる。http://trust.salesforce.com/trust/assets/pdf/Misc_SysTrust.pdf

7 OpenIDとは、URL形式で構成されたユーザーの身元確認をするためのID情報のこと。発行されるOpenIDでは、ユーザー名はURLアドレスとなり、さらにパスワードはOpenID提供サーバに保管されているので、他人と同じIDやパスワードを使用せずに、安スパムメールや不正アクセス等の心配がなく、安全にアクセスできる。

8 ネットワーク上で、シングルサインオンを提供することを目的とする標準化・技術開発のためのコンソーシアム。Sun Microsystems社がマイクロソフトの「.NET Passport」構想に対抗して立ち上げたもので、AOL Time Warner社、NTTドコモ、Hewlett-Packard社、VeriSign社、Bank of America社、Visa International社などを含め数十社が参加している。

ら切り離し「フェデレーション」を専門に請け負う事業者が成立するであろう。シングルサインオンが個々のID情報とパスワードを共通のものに置き換えるだけで、各サービスにアカウント情報が相変わらず分散しているのに対し、ID情報とパスワードの照合を一元化して認証のサービス間連携を実現するものである。シングルサインオンとフェデレーションの違いを**図5.2**に示すように、後者は認証行為そのものをアイデンティティプロバイダに任すものである。

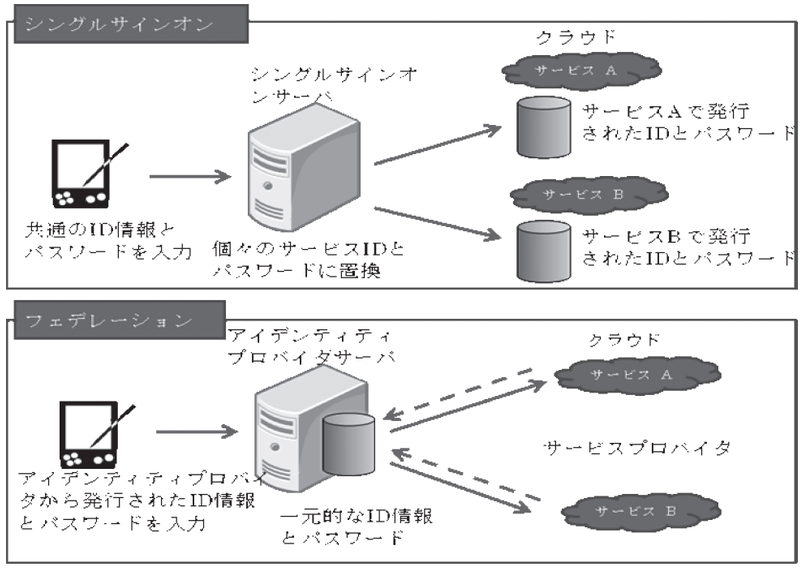


図5.2　シングルサインオンとフェデレーション

参考：ノークリサーチ（2010年）

また、本当の脅威はWebサイトが改ざんされることではなく、ID情報が盗まれていることだと再認識することも必要である。それには、まず使用するサービスのSLA（Service Level Agreement）を確認し、課金状態を定期的に（できれば毎日）確認し、一定以上の金額を使用していないかもチェックする必要がある。

とは言ってもデジタル家電などは家族間で利用するので、個人認証はできたとしてもヒューマンエラーによるリスクは残る。外出先から制御する場合、想定内のヒューマンエラーについては予め防護ソフトが組み込まれているとしても、想定外の使用法に対する処理は、性善説に立った子供を含む個々の家庭内のセキュリティポリシーを設定・遵守するしかないだろう。

5.5　外部統制の必要性

従来よくつかわれる内部統制とは、財務会計分野からの言葉であるが、1990年代になると会計統制以外に、コンプライアンスや経営方針・業務ルールの遵守、経営および業務の有効性・効率性の向上、リスクマネジメントなどより広い範囲が対象となり、一般的なコーポレート・ガバナンスのための機能・役割という側面を強めている。従来、外部委託におけるセキュリティ管理があった。外部委託業務についての内部統制については、セキュリティの確保を含めて、米国SOX法においても日本版SOX法においても委託元が責任を持つ必要がある。そこで、委託元に可能なのは、SLAによる基準の策定と定期的なレビューくらいである。委託先における業務プロセスの内部統制の状況を、委託元の企業や監査人が直接監査することもあり得る。そこで、外部委託作業における内部統制の監査を効率化するための枠組みがあり、これが前出のSAS70と呼ばれているものである。日本でも同様の基準として日本公認会計士協会の監査基準委員会報告書第18号「委託業務に係る統制リスクの評価」（通称「18号監査」）がある。委託元企業は委託先企業から受け取ったSAS70報告書をもって、外部委託業務についての内部統制の評価と代替することができる。換言すれば、外部委託した業務については内部統制の評価も外部委託が可能になるということになる。

クラウド時代にはユーザーのデータをクラウド業者が全面的に預かる立場から、この枠組みを使うことにすれば、**図5.3**のようになる。

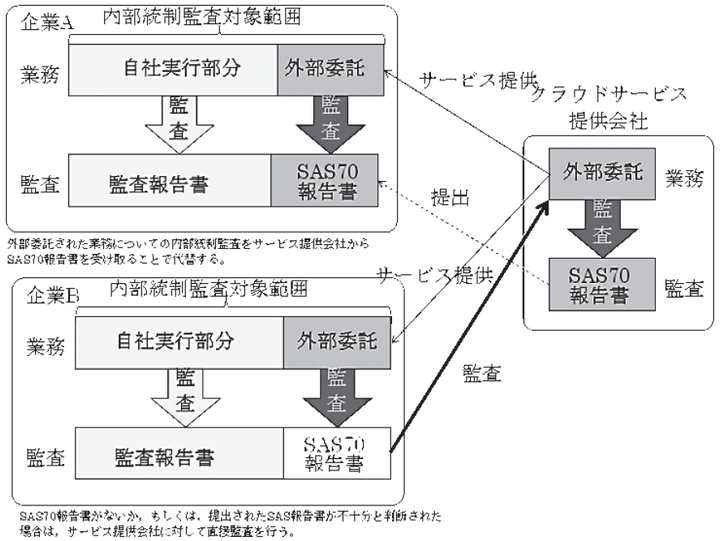


図5.3　SAS70のコンセプト

（中島浩光「第7回日本版SOX法に必要なセキュリティポリシーとは？」参考）

これは外部と係るため外部統制ともいうべきものである。クラウドのサービスに対しては、情報セキュリティ監査制度[9]がある。

それには、クラウド利用者がクラウド・コンピューティング環境のセキュリティレベルを比較検討することができるよう、クラウド事業者がセキュリティ対策の概要を表明するための標準様式を検討し、この様式に準拠した情報公開を促進する必要がある。このようにクラウド事業者のセキュリティレベルに一定の保証を与えるために、既にある情報セキュリティ監査制度を利用する方法が考えられる。また、短期的には、クラウドセキュリティにおける監査基準や認定制度、業界標準が求められる。長期的にはSLAや調達基準などにより、セキュリティがクラウド採用の阻害要因となるのは減少していくであろう。

5.6　データ越境移動の円滑化

国際的なデータの流通を見据えて、個人情報の円滑な越境移動を可能とするため、国際的な協調関係も検討していく必要がある。いわゆる越境データ流通（TDF）問題は、OECD（経済協力開発機構）において、約30年以上前から活発な審議が行われ、1985年4月の閣僚理事会で「Trans Border Dataflow宣言」が既に採択されている。ここへ来て、クラウド・コンピューティングの普及により、このTDF問題は、より現実的な解が求められるようになった。また、データの外部保存に関する制度整備と技術開発を行い、個人情報関連情報以外のデータについても、国内外のデータセンタへデータの種別に応じてデータを安全かつ円滑に移動・保存できるようにするための制度整備を検討するとともに、必要な信頼を形成するための技術開発を推進する必要が出てきた。

関係する法律等として、米国愛国者法（USA Patriot Act)、EUデータ保護指令（Data Protection Directive)、外国為替および外国貿易法、不正競防止法（独禁法）などがある。当面、SLA等でデータの扱い方を明確に指示するとともに、自社のセキュリティポリシーも明確に設定して自己防衛する必要がある。その際国際標準を決め、それに則って日本へも取り入れることが重要である。

9　情報セキュリティ監査制度は、情報セキュリティマネジメントをはじめとした情報セキュリティ対策の評価を、独立かつ専門知識を持った監査人が行う制度であり、2002年経済産業省告示第246号で創設、2003年2月1日から適用された制度である。情報セキュリティ監査基準に関するドキュメントの参照先は、http://www.meti.go.jp/policy/netsecurity/audit.htm である。

5.7　おわりに

クラウド時代の情報セキュリティについて2009年9月実施のあるアンケート結果の事例では、9割以上の人がセキュリティを気になる点として挙げている。「事業者がどのようなセキュリティ対策を実施しているのか知りたい」「事業者に対してセキュリティへ監査などによる、客観的な評価指標がほしい」が同率で1位になった。このほかに要望・意見などとして、①海外の法律適用範囲が不明確だが、国際法などグローバルでの基準が明確にされれば問題はないと思われる ②クラウド時代のNDA（Non-Disclosure Agreement：秘密保持契約）利用規約をIT業界として標準化し、保険の対応なども予め明確化して、クライアントの決断を早める対策を考えてほしい ③企業としてどの程度までセキュリティを確認すれば、利用者として情報管理に係る責任を果たしていることになるのか尺度（基準）を明確にしてほしい ④アクセスログやイベントログなどについて、どのくらい提供してもらえるのかが知りたい。などがあった。（富士通ジャーナルアンケート結果「クラウド時代の情報セキュリティ」)。また、情報システムコントロール協会（ISACA）の2010年4月の調査によると、米国のIT専門職（1,800名）の半数近く（48%）がクラウドは、メリットよりリスクが大きいと回答したと言う。

今後こうした不安感をなくすためにも、組込み開発においても、クラウド時代に即応したIT統制が不可欠になる。また、そのための基準やガイドラインと言った標準的なものが早急に整備されることが望まれる。

■参考文献

1) 経済産業省「クラウド・コンピューティングと日本の競争力に関する研究会」報告書、2010年8月16日
http://www.meti.go.jp/press/20100816001/20100816001-3.pdf

2)「富士通ジャーナルアンケート集計結果：テーマ「クラウド時代の情報セキュリティ」2010年9月

3) 岩上由高「第2回クラウド活用時に考慮すべき7つの課題と対策」ノークリサーチ 2010.10.3

4) 情報マネジメント ＞ IT戦略 ＞ 連載：セキュリティツールで作る内部統制「第7回 日本版SOX法に必要なセキュリティポリシーとは？」
http://www.atmarkit.co.jp/im/cits/serial/soxfw/07/01.html

5) 済賀「組込みシステムのセキュリティ対策」都立産業技術研究センター「技術セミナー」2009.7.3

第6章
組込みシステムのセキュリティ

近年、インターネットの急速な普及に伴い、本来クローズされたプラットフォームを採用することが多かった組込みシステムもネットに接続され、外部からの攻撃にさらされる機会も飛躍的に増えている。その為セキュリティ対策が過去とは比較にならぬほど重要視されるに到っている。

JASAでは2010年10月15日JASA/ETセミナーの一環として、情報処理推進機構（IPA）様より3氏をお招きし、「組込みシステムのセキュリティ」の現状、研究成果、脅威などについてお話いただいた。

本章はその講演をベースにレポートにまとめたものである。
講師の方々の氏名と演題は以下の通りである。

「組込みシステムのセキュリティ調査報告　～自動車 ・ 情報家電 ・ 制御システム～」
講師　中野 学 氏（情報処理推進機構）

「組込みシステムにおける最近のセキュリティ脅威等の紹介」
講師　小林 偉昭 氏（情報処理推進機構）

「組込みシステムのセキュリティへの取組みガイド」
講師　萱島 信 氏（情報処理推進機構）

6.1　組込みシステムのセキュリティ調査報告
～自動車 ・ 情報家電 ・ 制御システムなど～

本節は、IPA情報セキュリティ技術ラボラトリー主任の中野学氏のご協力を得て、レポートにまとめたものである。

6.1.1　組込みシステムのセキュリティ

一口に組込みシステムといってもその対象の範囲は、小はRFIDや携帯電話から大は制御システムまで非常に広い。ここでは情報家電、自動車、制御システムの3つの分野のセキュリティを対象として議論を進めたい。

IPAは2006年から組込みシステムのセキュリティの調査を開始した。従来PCとは異なり組込みシステム機器はスタンドアローンでの使用が主であったものが、ネットワークに接続する機能を有することで、悪意あるユーザの攻撃による被害の可能性が一気に大きくなり、セキュリティ対策が重要になってきたからである。

(1) 組込みシステムセキュリティの特殊性

PCの場合であれば事前にアンチウィルスソフトウェアの導入 ・ セキュリティファイアウォールの利用等で対策が実施可能である。もし、ソフトウェアに脆弱性が発見されたとしてもセキュリティパッチのダウンロード等で対応することができる。一方で、組込みシステムの場合は、開発環境や製品の特徴等の違いの他にリソースの制約から、PCと同じような対策を実施するのは困難である。また、利用者（ユーザ）が攻撃目的で組込みシステムを解析する可能性も存在する。例としてリバースエンジニアリングなどが典型的なものである。

(2) 具体的なセキュリティ課題

組込みシステムのライフサイクルに応じて次のような対策を具体的に立てることが大事である。

①企画段階　セキュリティ対策ガイドラインの策定をし、一貫したセキュリティ対策を立てること

②開発段階　低リソースで利用できるセキュリティ技術の開発 ・ 利用を図り、セキュアプログラミング等によって製品のセキュリティを確保すること。

③運用段階　インシデント対応方法体制を確立すること。

④廃棄段階　廃棄方法の周知を徹底させること。

6.1.2　情報家電と自動車の情報セキュリティ

情報家電の世界の特徴として、様々な機器がネットワークを介して繋がるため、その全体像が特に一般人にとっては非常にわかりにくい事があげられる。どのような機器がネットワークにつながっているのか、ネットワークからどのような情報が来るのか、それらの情報は全て信頼できるのか、一般の利用者が理解するのは至難である。また、一方どのような情報が出て行くのか、それはどのように利用されるのかも解らずに利用していると、情報漏洩に繋がる可能性もある。これは自動車の世界でも同様のことが言える。

(1) 守るべき対象（情報等資産）

守るべき対象は、情報家電や自動車に含まれる情報だけでなく、組込み機器から外部に出て行く情報、ネットワークを介したサービス、さらには組込み機器本体までを含める。これらを総括して、「情報等資産」と呼ぶ。車の場合、直接人身に危害を及ぼす可能性が高いので「情報等資産」には実態上人身を含めてもよいであろう。

(2) 情報家電に対する脅威

情報家電本体に対する攻撃は、以下の５パターンに分類できる。

①「直接、入出力」での攻撃。利用者自身やにせの点検員等による攻撃。

②「宅内ネットワーク経由」での攻撃。家族や同居人のミスを含めた攻撃。

③「持込機器経由」での攻撃。外部から持ち込んだUSBメモリ等による攻撃。

④「広域ネットワーク（電話回線）経由」での攻撃。

⑤「広域ネットワーク（インターネット）経由」での攻撃。

(3) 自動車に対する脅威

自動車の場合、特にインフォテインメント系では同じことが言え、以下の３パターンに分類できる。

①「近接」での攻撃。整備員なりすましや停車時の車に対する攻撃。

②「中間（持込機器着脱等）」での攻撃。持込みのカーナビ等による攻撃。

③「広域ネットワーク（インターネット）経由」での攻撃。

上記をまとめたものを図6.1、図6.2に示す。

情報家電に対する脅威の例（情報家電周辺）

IPA

情報家電分類 ＼ アクセス経路	設備系	白物系	AV系
直接、入出力	・居住者なりすましによる攻撃（ドア錠等） ・点検員なりすましによる外部アクセス用設定情報の詐取（ホームゲートウェイ）	研究会では特に重要な脅威が挙げられていない	・家電店員による外部アクセス用設定情報の漏えい（Web力メラ等）
無線LANやPLC等で宅内で繋がる	・宅内ネットワーク経由で侵入、乗っ取り（ホームゲートウェイ） ・盗聴による個人情報漏洩（宅内ネットワーク上）	・宅内ネットワーク経由で侵入しOS・アプリケーションを改ざん ・盗聴による個人情報漏洩（宅内ネットワーク上） ・中古家電でウィルス感染（同）	・宅内ネットワーク経由で侵入しOS・アプリケーションを改ざん ・盗聴による個人情報漏洩（宅内ネットワーク上） ・中古家電でウィルス感染（同）
家庭に持ち込んでPCと繋がる	現状では対象が少ない		・着脱機器によるウイルス感染 ・持ち出した家電の盗難、情報漏洩（着脱機器上） ・コンテンツの違法コピー（同）
電話回線で外部と繋がる	研究会では特に重要な脅威が挙げられていない		
インターネットで外部と繋がる	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）	・乗っ取り、踏み台 ・通信機能の停止（DoS） ・OS・アプリケーション改ざん（情報家電）

図6.1　情報家電に対する脅威の例

自動車に対する脅威の例（自動車周辺）

IPA

自動車機能分類 ＼ アクセス経路		制御	インフォテインメント
		セーフティ上クリティカル ⟷ セーフティ上影響小	損害大（金銭、個人情報等） ⟷ 損害小
近接		不正ECU取付けパラメータ改ざんプログラム改ざん（駆動系ECU） 他人のETCカードに成りすまし	個人情報の吸い出し、プロファイリング、プログラム改ざん（エンタメ系ECU）
中間（持込機器着脱等）		運転情報の破壊、改ざん、漏洩（ドライブレコーダ）	・持込機器からエンタメ系ECUへのDoS攻撃、無線へのDoS攻撃 持込機器からウィルス感染
広域ネットワーク経由	専用	サーバなりすましによる虚偽メッセージの表示（車車間（路車間）通信）	エンタメ系ECU・車載ネットワークへのDoS攻撃
	汎用	研究会では特に重要な脅威が挙げられていない	決済情報フィッシング・盗聴 虚偽情報の表示、ウィルス感染、インフォテインメント系ECUや通信機能へのDoS攻撃

図6.2　自動車に対する脅威の例

6.1.3　それぞれの脅威の特徴

(1) 情報家電における脅威の特徴

情報家電における脅威の特徴としては、以下のような可能性があげられる。

a) 高齢者 ・ 子供などの情報リテラシーが充分でない利用者が存在する可能性。

b) 情報等資産の多種多様化、範囲拡大の可能性。

c) オークションによる転売や譲渡による情報の漏洩の可能性。

d) セキュリティ対策が不十分な情報家電が混在する可能性。

e) 何が繋がり、誰が利用しているか、把握できなくなる可能性。

f) 着脱機器やテレメトリングによる情報の拡散の可能性。

g) 偽のダウンロードパッチを受け入れてしまう可能性。

h) 情報家電経由でインターネットの不正サイトにアクセスしてしまう可能性。

i) 宅内ネットワークのセキュリティ設定が行われていない可能性。

これらは、情報家電がネットワークに繋がる事により、情報や機器が脅威がにさらされる可能性を示している。

j) 第三者の侵入による不正な設定変更の可能性

k) メーカ点検員になりすました第三者による不正な設定変更の可能性

l) 利用者自身による改造の可能性

これらはいずれも情報家電自体に対する直接的な攻撃が可能であることを示すものである。

(2) 自動車における脅威の特徴

同様に自動車における脅威の特徴は以下の可能性があげられる。

a) 情報等資産の多種多様化、範囲拡大の可能性。

b) オークションやレンタルによる情報の漏洩等の可能性

c) セキュリティレベルが低い組込み機器が混在する可能性

d) 移動先で何が繋がり、誰が利用しているか分からない可能性

これらはいずれも自動車の利用方法の多様化によって脅威が拡大する可能性を示し、

e) 着脱機器やプローブによる情報等資産の拡散の可能性

f) 偽のダウンロードパッチを受け入れてしまう可能性

g) カーナビ経由でインターネットの不正サイトにアクセスしてしまう可能性

これらは自動車が外部ネットワークを利用したサービス等と繋がる事で脅威が発生する可能性をしめすものである。

h) 駐車場等での第三者による不正な改造の可能性

i) メーカ点検員になりすました第三者による不正な改造の可能性

これらは過去から物理的には可能な事であったが、車載ソフトウェアの脆弱性等によってブレーキ等に影響が出るのであれば、重大な脅威になりうる。

j) 利用者自身による改造の可能性

自動車の愛好者等にとっては、自車のチューンナップ等を目的として車載ソフトウェアに手を入れる事で、ソフトウェア上の新たな脅威が発生する事や、既存のセキュリティ対策が欠損する可能性もある。

k) 重大な被害即ち人命にかかわる被害が起きる可能性

l) 社会的混乱を招く可能性のある偽交通情報

また、自動車は社会インフラの一つとなっており、セキュリティ上の課題が社会的な脅威に結びつく可能性もある。

6.1.4　情報家電と自動車のセキュリティ対策の方向性

まず以下に述べるような対策をその第一歩とする。

(1) 利用者にセキュリティ対策を施す意識、被害に気づく知識をもたせるとともにセキュリティ対策にコストをかける文化を醸成すること。

(2) メーカやサービス提供企業に充分なセキュリティ対策を働きかけると同時に情報家電のセキュリティ対策に関連した制度やしくみを充実させること。

(3) 利用者一人ひとりに何が繋がっているか、誰が利用しているかを明らかにし、セーフティとセキュリティの連携により安全 ・ 安心を実現すること。

これらの実現のためにも中期目標をしっかりと立て、一歩ずつ前進を心がけるべきである。例えば、組込みシステムにセキュリティを取り入れる事を検討する一方で、利用者にもセキュアな製品を選ぶ意識を育てることで、情報家電のセキュリティが一般に浸透するものと考えられる。

6.1.5　制御システムセキュリティ

IPAでは2008年より制御システムのセキュリティ調査を行っている。

制御システは情報系システムと制御系システムの二種類に大別できるが、今回の発表は主に後者に絞ったものである。

6.1.6　制御システムのセキュリティ課題

大別して以下の3つの課題があげられる。

課題1 ： オープン化に伴う脆弱性リスクの混入

汎用製品、標準プロトコルネットワーク採用により、これまで情報システムで発生していたような既知の脆弱性が存在するリスク、ワームなどのウイルスの侵入や、機密情報漏えいのおそれが最近急激に増大している。

課題2 ： 製品の長期利用に伴うセキュリティ対策技術の陳腐化

制御システムは通常10 〜 20年使用が前提であり、開発時のセキュリティ対策の効果が陳腐化する可能性がある一方で、パッチ等により最新の対策を施そうとしてもハードウェ

アが対応できない可能性がある。

課題３ ： 可用性重視に伴うセキュリティ機能の絞込み

可用性重視の観点から、一般的に、システムや通信上の負荷となるウイルス監視やファイアウォール設置等の実施が困難である。また、セキュリティパッチや新規セキュリティ系システム設置の際には、PC等の情報機器と違い、一分一秒たりともとめられない制御システムでは再起動等の処置ができない可能性がある。

6.1.7　制御システムのセキュリティに関わる取組みのポイント

2009年度の調査では、欧州や米国の制御システムセキュリティについて、制御システムセキュリティの評価検証、制御システムに関わる製品の認証、脆弱性共有等のためのデータベース、制御システム関係者を助けるガイド、ツールの四つの視点から調査を行い、日本の制御システムセキュリティの現状を含めて表にまとめた（**図6.3**）。

日米欧の取組み状況比較は下表に示すとおりであるが、海外では制御システムのセキュリティ対策についての検討が進められており、日本においても参考となる可能性がある一方で、制御システムの海外展開等を考える上では、これらの情報を参照する必要がある。

取組み状況調査結果のまとめ

● 日米欧の取組み状況比較

IPA

施策	欧州	米国	日本
ガイド・ツール	・推奨されるプラクティス集（Good Practice）を公開（英国CPNI、オランダTNO水セクター向け） ・セキュリティ基準を策定（ドイツBSI standard 100-1～4） ・自己評価ツールを配布（英国CPNIのSSAT） ・情報共有の仕組みを整備（欧州のE-SCSIE、英国CPNIのSCSIE、スウェーデンSEMAのFIDI-SC）	・推奨されるプラクティス集（Good Practice）を公開（DHS/CSSP） ・セキュリティ基準を策定中（NISTのSP800-82およびISAのISA99 100、NERCのCIP002～008） ・自己評価ツールを配布（DHS/CSSPのCS2SATおよびその後継のCSET） ・情報共有の仕組みを整備（2008年までPCSF、2009年よりICSJWG）	・「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定に当たっての指針」（2007年6月 情報セキュリティ政策会議）などに基づき分野ごとに安全基準を設定 ・独自のツール類は少ない
評価・検証	・ヨーロピアンテストベッド取組みの一部としてIPSCではSCADAテストベッドを開設しセキュリティ検証を実施	・DOEがSCADAテストベッドを開設しセキュリティ技術の開発、検証を実施	・電力中央研究所で制御システムセキュリティの評価・検証を行っているが、事業者または制御機器ベンダー内で共通的に利用可能なセキュリティテスト環境等は少ない
データベース	・CPNIが制御システムセキュリティプログラムのひとつであるSCSIEを運営しており、インフラ運用者間での脆弱性情報共有カンファレンスを定期的に実施 ・制御機器ベンダーが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る ・TNOがインシデント情報のデータベースを構築	・US-CERTが制御システムの脆弱性関連情報のデータベースを持つが15～20件と少数 ・RISIが制御システムのセキュリティ事象データベースを運用 ・制御機器ベンダーが脆弱性関連情報をユーザグループに直接通知、対策し、ユーザグループ内での解決を図る	・JPCERT/CCが制御システムの脆弱性関連情報の収集、公開を実施。但し件数は少ない ・IPAが脆弱性対策情報DB（JVN iPedia）を運用
認証	・TUViTが複数の基準を顧客要件により組み合わせ、制御システムの監査・認証を実施	・製品認証機関による認証製品を利用することで、一定のセキュリティレベルが担保されていることを確認、保証可能	ー

図6.3　国内外の制御システムセキュリティ施策の比較

6.1.8　調査分析結果

上記の調査分析の結果をまとめると欧米のセキュリティ対策の実状は以下のようになる。

(1) ガイド・ツールに関しては、セキュリティ基準の策定、推奨プラクティス集の公開、自己評価ツールの配布を実施している。

(2) 評価・検証に関しては、SCADAテストベッドの開設によるセキュリティ検証を実施している。

(3) データベースに関しては、制御システムのインシデント情報のデータベース構築・公開を開始、認証に関しては、民間主導によるセキュリティ監査・認証サービスが行われており、ISA ISCIによる標準化が進展中である。

(4) 制御システムセキュリティ強化に向けた認識向上や関係者間の信頼関係構築により施策の普及を促進させるための、情報共有コミュニティを設置し運用するなど脆弱性対策への取組みが拡大中である。

一方、日本としても具体的な対策を進める必要性があるが、その実状は：

(1) 日本独自のガイド・ツール類の提供はまだ少なく、テスト環境も一部セクターのみである。

(2) 脆弱性対策情報（JVN iPediaなど）のデータベースはあるがインシデンツを含む幅広い制御システムセキュリティの情報収集はこれからという状況にある。

制御システムのセキュリティ対策のあり方は日本と欧米とで必ずしも同一ではないが、日本の重要インフラにとっての優先度を判別した上で、最も効果のある課題から始めていくことが必要であり、セキュリティ規格標準化の動向に関しては、産業の国際競争力強化の観点からは日本独自の規格ではなく、国際標準への対応を念頭に推進することが重要であると考えられる。

他方、欧米での制御システムセキュリティへの取組みも、まさに現在進行形であり、わが国としては、今後の動向を注視しながらアジアの展開も視野に幅広く対応すべきである。制御システムセキュリティの脆弱性対策においては、関係者の認識改善と対策の実効性向上の観点からも、官民連携による情報共有の仕組みづくりが鍵であるといえよう。

6.1.9　今後の検討課題

今後の検討課題をまとめると以下のようになろう。

(1) 利用者、メーカ、サービス事業者等の情報リテラシーを向上させること。

利用者の情報セキュリティのリテラシー向上、対策コストの必要性の理解を促進させるとともに、リテラシー向上が難しい利用者を誰がどのように保護するかの方策を検討するとともに、関係企業に対するガイドライン、利用者向け説明資料の整備、配布を急ぐこと。

(2) 状況の可視化と役割分担の明確化を実現すること。

不正な機器の接続や不正利用の発見・対策を行う可視化のしくみの実現をはかるとともに、セキュリティ上の脅威に対する役割分担や、自動車や家の「物理的なバリア」と「ネットワーク上のバリア」のあり方の明確化をはかること。

(3) ライフサイクルを通じた検討をおこなうこと。

設計段階からのセキュリティ検討、廃棄時の個人情報やセキュリティ機能の適切な消去などライフサイクルを通じた検討をおこなうこと。

(4) 協力および提言の場の確立

利用者、メーカ、サービス事業者、セキュリティ技術者が協力し、セキュリティ対策を検討するとともに、法制度の整備について国に提言していく場を設置すること。

(5) ネットワークの両側でのセキュリティ対策の実施

機器側（メーカ側）とサービス側（サービス提供企業側）の双方でのセキュリティ対策による、より確実な脅威の解消をはかること。

以上の5項目があげられるであろう。

6.1.10 安全な組込みシステム社会にむけて

安全な組込みシステム社会の実現のためには以下の考察が重要であろう。

(1) 組込みシステムの特徴（省電力、低リソース、等）を考慮した上で、従来の情報システムのセキュリティインシデントやその対策についてのセキュリティに関する考察を深めること。

(2) 組込みシステム間の相互接続や融合時の複合的な環境でのセキュリティに関する考察を行うこと。

(3) 利用者の個人情報、金銭被害に繋がる情報、さらに人命に繋がる情報等、取扱う情報資源の特徴の観点を考慮に入れた考察を行うこと。

(4) 組込みシステム開発者・技術者のセキュリティを含めた意識共有の為の活動を進展させること。

以上のような様々な観点から課題を検討すると同時に、組込み開発者やユーザ、事業者、セキュリティ研究者といった組込みシステムに係る人々の連携で、課題の解決に向けて取り組むことが何よりも重要であろう。

6.1.11 IPAの活動の紹介

最後に組み込みセキュリティに対するIPAの活動を図6.4にまとめた。各種の調査の他に検証ツールなども公開しているので、関係者の方々に是非活用していただきたい。

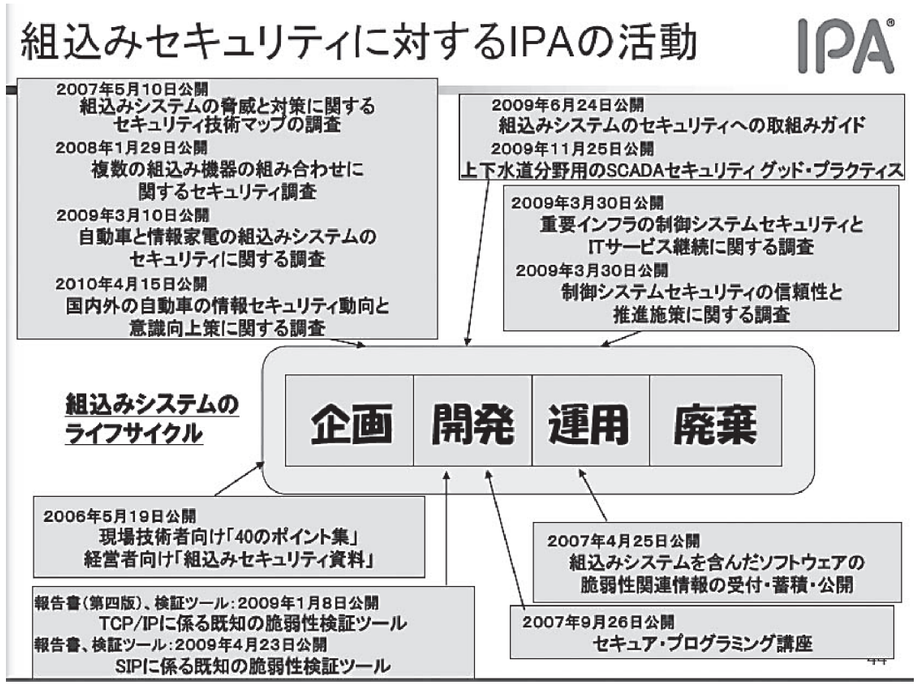


図6.4 組込みシステムセキュリティに対するIPAの活動

6.2　組込みシステムにおける最近のセキュリティ脅威等の紹介
～自動車 ・ 情報家電 ・ 制御システムなど～

本節は、IPA情報セキュリティ技術ラボラトリー長の小林偉昭氏のご協力を得て、レポートにまとめたものである。

6.2.1　情報セキュリティ技術ラボラトリーの紹介

IPAは80%以上の人が民間出身の人で構成されており、民間との情報交換により民間に役に立つ事を進めているので、積極的に利用して頂きたい。

情報セキュリティ技術ラボラトリーは主として「脆弱性対策」、「新分野のセキュリティ対策」に付いて活動している。（**図6.5**参照）

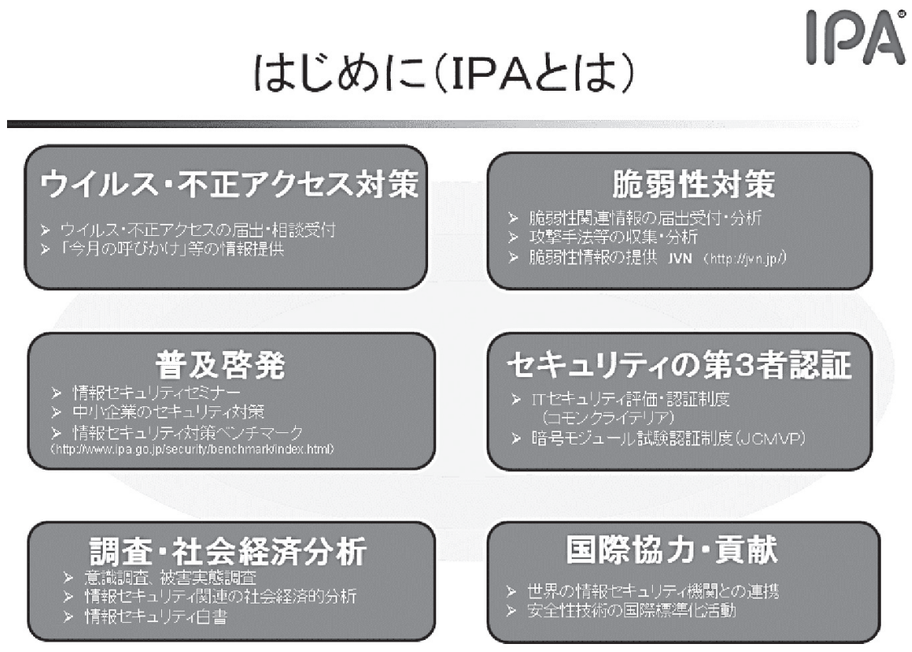


図6.5　初めに（IPAとは）

本稿では、組込みシステムのセキュリティに付いての米国の論文を中心に脅威と対策について解説する。

6.2.2　セキュリティ脅威の現状と対象の変化・多様化

1）インターネットの初期は「いたずら」程度であったが、現状は「金銭 ・ 犯罪 ・ テロ ・ 情報戦など」と攻撃（悪意）の動機が変化してきている。

IPAの定点観測では、期待していないアクセス（攻撃？）は、2010年8月1ヶ月で162の発信元から358件のアクセスがあり、世の中のPCが約4分ごとに期待していないアクセス（攻撃？）にさらされている事になる。

2）多様化する脅威

社会の変化に伴いセキュリティ脅威も多様化しており、米国の９１１同時テロのような社会政治的なもの、内部不正ほか脅威の対象が拡大している。（**図6.6**参照）

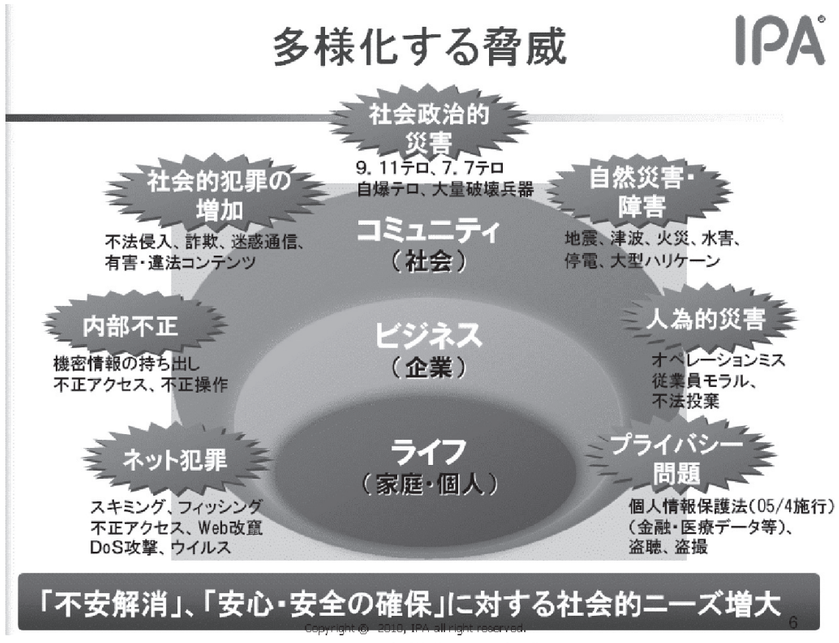


図6.6　多様化する脅威

3）脅威と危険性（リスク）と影響

昔と今のサイバー攻撃の攻撃構造と手法と影響の変化に対して、「脅威」に対する対策を考える上で、「危険性」と「影響」を十分に検討する必要がある。

また、セキュリティ製品による対策を取るケースも増加しているが、システムの設計思想を変化させないと攻撃の変化に対応できなくなる。（**図6.7**参照）

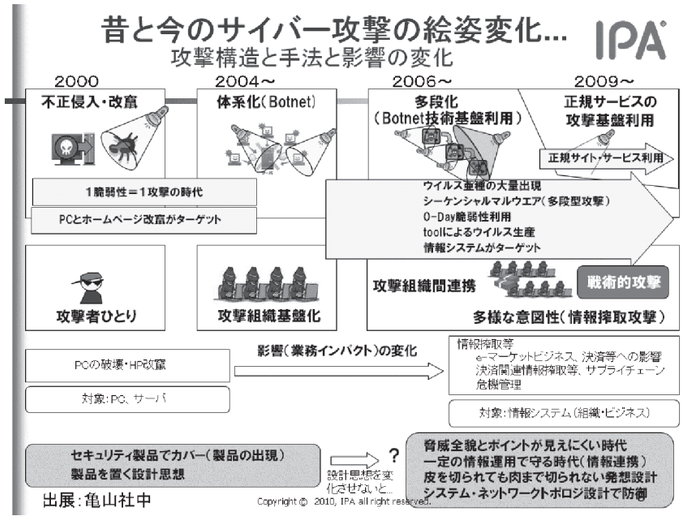


図6.7　昔と今のサイバー攻撃の絵姿変化

6.2.3　サイバー空間(新しい生活空間？)

インターネットの高速化と普及に伴いサイバー空間が広がり社会的な影響度合いが高度になってきており、愉快犯→金銭犯→エスピオナージ（産業スパイ）→国防の対象となってきた。

リアルとサイバーの信頼関係を強め連携強化により攻撃から防御する事が重要となっている。(**図6.8**参照)

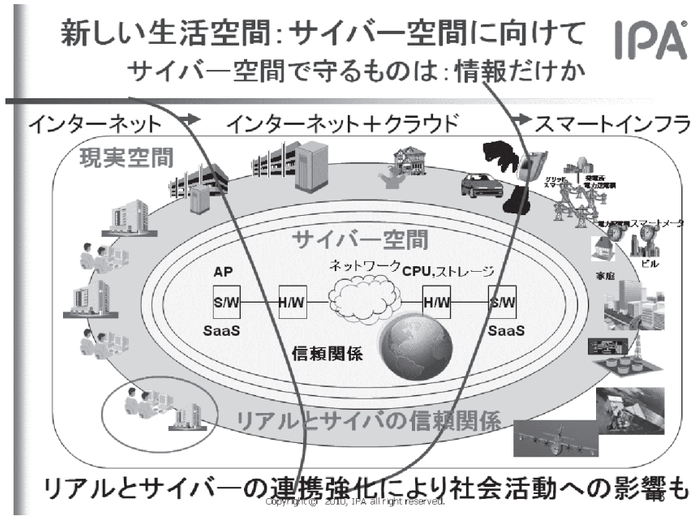


図6.8　新しい生活空間 ： サイバー空間に向けて

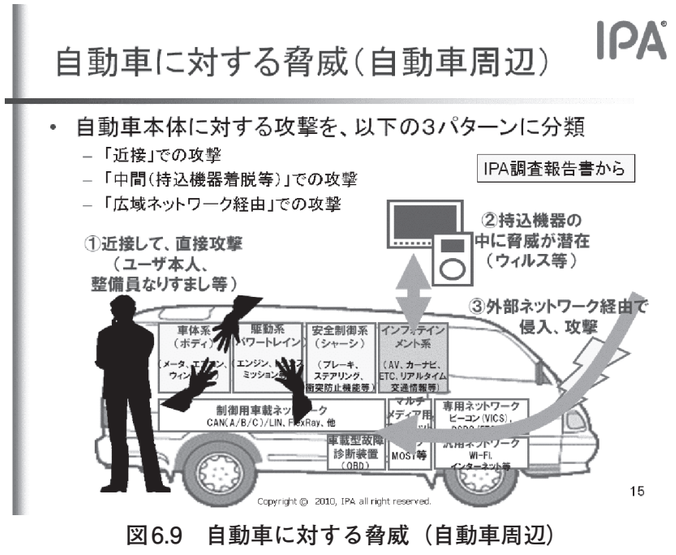
6.2.4　組込みシステムのセキュリティ脅威 自動車に対する脅威（自動車周辺）

自動車本体に対する攻撃を、IPAでは以下の３パターンに分類する。(**図6.9**参照)

①「近接」での攻撃

②「中間（持込機器着脱等)」での攻撃

③「広域ネットワーク経由」での攻撃



15

図6.9　自動車に対する脅威（自動車周辺）

6.2.5　最新自動車に対するセキュリティの現状の実験論文紹介（その１）

論文 : Experimental Security Analysis of a Modern Automobile

http://www.autosec.org/publications.html

1) 安全性 ・ 信頼性に対して、現状ハード故障 ・ ソフトバグが検討の主対象であったが、今後は、セキュリティ攻撃により発生する障害などについての考慮が必要となる。

今回のセキュリティ現状に対する実験をするうえでの背景を次にあげる。

①自動車の組込システム

ECUが結合してきている。これは複雑･複合的な機能を実現するためで、CANやFlexRayなどの車載ネットワークで接続されている。

安全性重要システムは、それぞれ独立だが、現実はブリッジで繋がっている。

・ テレマティクスサービス

・ GPSの利用でサービス拡充　故障位置、盗難車対策

②関連した研究 ・ 事例

研究 ： セキュリティとプライバシー、CANプロトコルのセキュリティ

マーケット ： 車好きのチューニング

軍事（DARPA）： 完全無人自動車

③脅威モデル

攻撃者が外部のネットワークから内部ネットワークへ攻撃

物理アクセス攻撃：（メカニシャン、駐車ヴァレット、レンタカー、家族、人・・・）OBD-IIポート（ダッシュボードの下）、偽造品や悪意の部品

多様な無線インタフェースからの攻撃

2) 自動車は複数のECUとその他のモジュールとがネットワークで繋がっており、単独の装置だけの対策では不十分で、全体としてのセキュリティ対策が必要である。（**図6.10**参照）

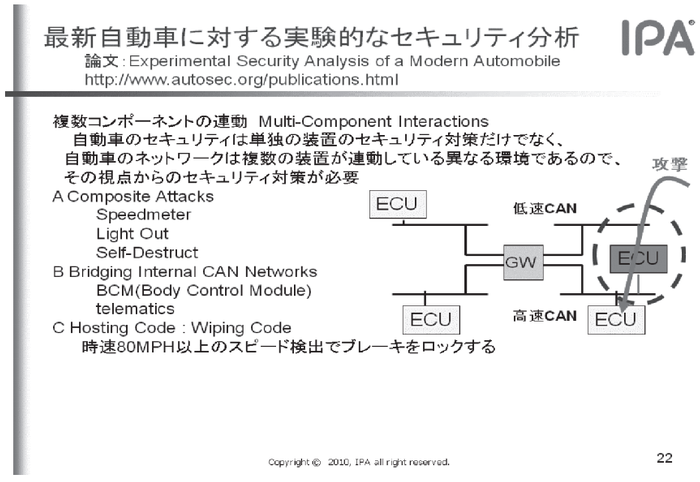


図6.10　複数コンポーネントの連動　Multi-Component Interactions

3) 最近の自動車の現実の脆弱性に関する予測の実験検証

実験検証は次にあげる事を前提として、多くの関係者の利害衝突の中で検討し、現実的で実際的なセキュリティ対策を作り上げる事が重要となる。

①Diagnostic and Reflashing Services

車のチューニング、サインドファームウエア更新、アクセスコントロールの欠如

②Aftermarket Components

外部フィルタリング装置、飛行機のブラックボックスのようなもの

（障害の切り分けログ、フォレンジック）

③安全性・信頼性から求めるハード故障・ソフトバグはセキュリティ攻撃の的にもなりうる。（**図6.11**参照）

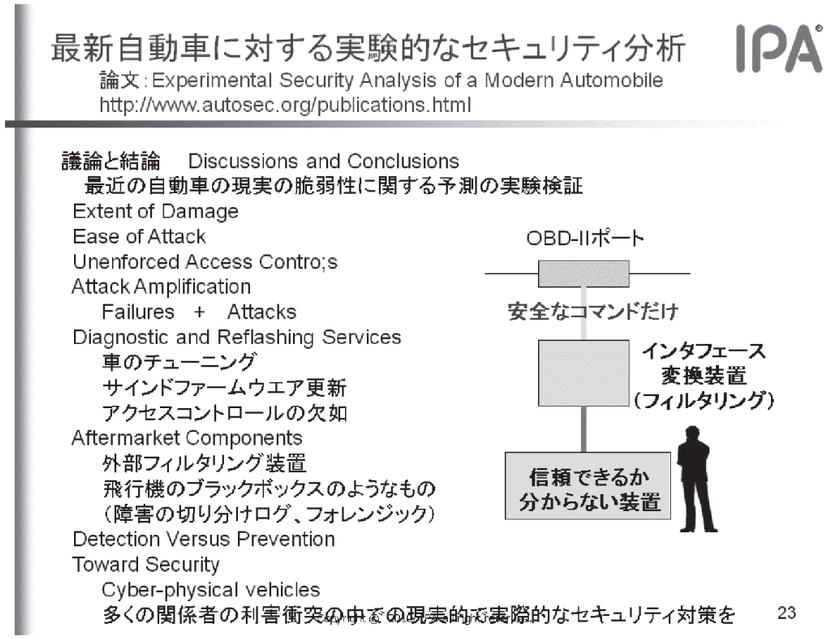


図6.11　自動車に対する脅威（自動車周辺）

6.2.6　最新自動車に対するセキュリティの現状の実験論文紹介（その2）

1) タイヤ空気圧警報システムへの攻撃実験

車内ワイヤレスネットワークの特徴。

①TPMとECU間のワイヤレス通信は、315MHzか433MHz HF(UHF)のASK(Amplitude Shift Keying)あるいはFSK(Frequency Shift Keying)モジュレーションを使用。

独自のプロトコル用いているが、ワイヤレスシグナルはインプットバリデーションや暗号化がされておらず、GNUラジオとUniversal Software Radio Peripheral (USRP)を使用すれば簡単に傍受できる。

②コミュニケーション可能範囲が広い。TPMSの場合、ローノイズ・アンプを使用すれば40m先までシグナルを受信できることがわかった。

そのため、対象となる車の横を走行している自動車から簡単にハッキングができてしまう。

実際に研究者たちは時速45キロで並走している車から、対象となる車へのリモート攻撃を行っている。

③タイヤ内部のセンサーは、それぞれのセンサー独自の32ビットのアイデンティファイアーを送信している。

このアイデンティファイアーを一度読み込めば、対象となる車の位置を特定することができ、個人のプライバシーの問題にもなってくる。

2) 走行中の車載ネットワークへのリモート攻撃に成功

これまで、自動車間、自動車とインフラ間通信のセキュリティは各種研究が行われているが、TPMSのような自動車内部のワイヤレスネットワークは遅れていた。

それは、

a) 車の金属ボディーがワイヤレスシグナルを遮断する

b) ワイヤレスシグナルを受信できる範囲が非常に狭い

と想定されていたためだ。しかし、今回の研究ではこの前提が覆されたことになる。

研究者らはTPMとECU間のプロトコルをリバースエンジニアリングして突き止めている。

それによれば、「大学の研究者レベルのエンジニアなら2～3日」で、「大学院レベルでも2～3週間」あればリバースエンジニアすることができたとしている。

また、これに使用された機器は総額1,500ドル程度だったそうだ。技術的にもコスト的にも簡単な攻撃と指摘されている。

今回の研究では、こうした脆弱性を悪用した攻撃が、TPMのシグナルをスプーフィングして偽の空気圧の値をECUに送信する程度にとどまっているが、初のリモートからの攻撃実証は、今後、車載搭載PCシステムへのリモートからの攻撃の増加を予測するものと言えよう。

6.2.7　スマートフォンと Jailbreak 文化の脅威

1) スマートフォン（iPhone、Android など）上のアプリは普通、制限された環境（檻、Jail）の中で動作するが、その環境を破るといきなりおおくの脅威に晒される。

2) また、脆弱性があれば利用者の意図とは無関係に檻を破られる事もある。

アプリの開発者はJailに頼らないセキュアーコーディングをしなければならない。

6.2.8　恐ろしい標的型攻撃と10大脅威

標的型攻撃はサイバー空間での産業スパイのようなものであり、個人レベルに関わらず盗聴 ・ 盗撮により企業からの金銭の搾取にもなってきている。

標的型脅威として

①特定の企業 ・ 組織を標的とした標的型攻撃が深刻化し、攻撃対象の組織 ・ 人が限定的。役員やキーの従業員にピンポイント攻撃する。

②攻撃が見えにくくなっており、近年のマルウエア攻撃は従来のマルウエアとは異なり一般的なセキュリティ対策では十分に機能しない。（多段型、ダウンローダ、脆弱性利用、検出 ・ 解析対策、攻撃対象が限定的、etc…）

③企業 ・ 組織は十分な情報や技術的解決策を得られない

攻撃発生前に情報を入手し対応する事が難しく、詳細な挙動 ・ 仕組みもよく分かっていない

これらの事から脅威を正確に把握できないので、マルウエア対策（検知 ・ 駆除）を見直

さなければならない。（**図6.12**参照）

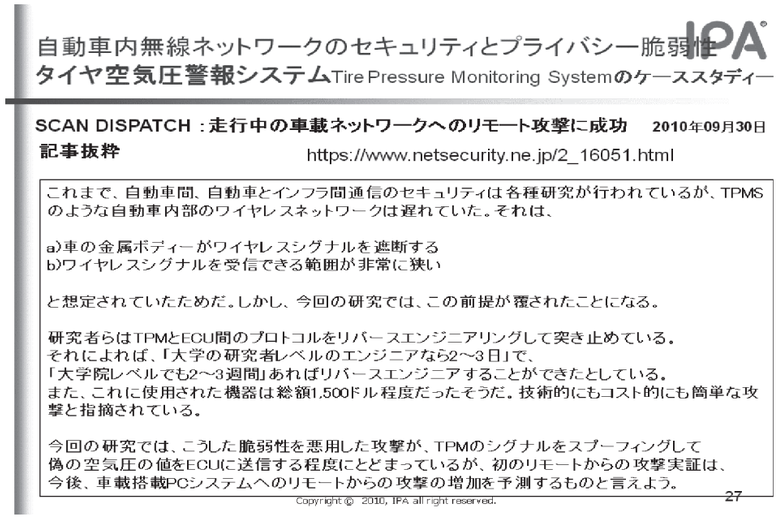


図6.12　近年の標的型攻撃

1) 攻撃者に対する挑戦と課題

①攻撃者側に攻撃を困難にするための準備 ： さまざまな解析対策や解析を困難にする。

②解析効率化ツール環境等の基盤整備と、有効な対策分析の為に脅威変化の継続監視が重要。（**図6.13**参照）

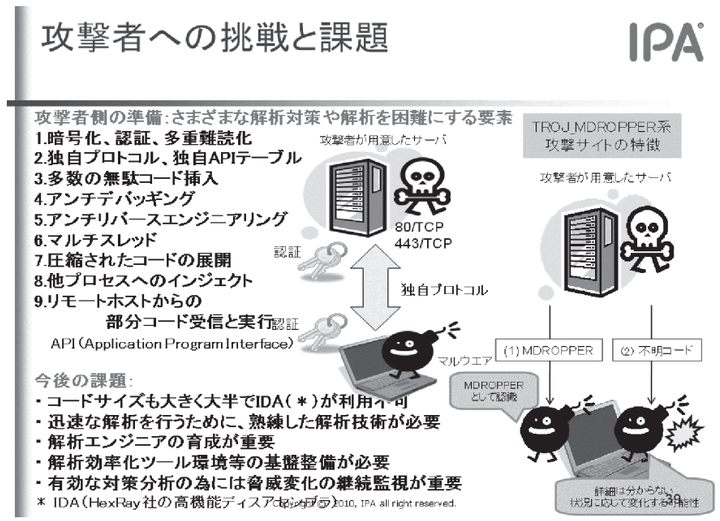


図6.13　攻撃者への挑戦と課題

6.2.9　１０大脅威「あぶり出される組織の弱点！」

「2010年度版 10大脅威」はIPAに届出のあったコンピュータウイルス、不正アクセスおよび脆弱性に関する情報や、インターネット等で一般に報道された情報を基に、「情報セキュリティ早期警戒パートナーシップ」に参画する関係者のほか、情報セキュリティ分野における研究者、実務担当者など120名から構成される「10大脅威執筆者会」でまとめたものをIPAが、2005年から毎年公開しており、今年で6回目となる。

今年の１０大脅威を次にあげる。

1位　正規のウェブサイトを経由した攻撃の猛威
2位　アップデートしていないクライアントソフト
3位　多様化するウイルスやボットの感染経路
4位　アップデートしていないウェブアプリケーション
5位　恒常化する情報漏えい
6位　巧妙化する標的型攻撃
7位　深刻なDDoS攻撃
8位　ユーザIDとパスワードの使いまわしていませんか
9位　クラウドのセキュリティ
10位 インターネットインフラを支える製品の脆弱性

6.2.10　対策について ： IPAからのプレゼント

IPAでは、「脆弱性を利用した標的型攻撃のための解析ツール」を開発しているので、大いに利用し活用したい。（**図6.14**参照）

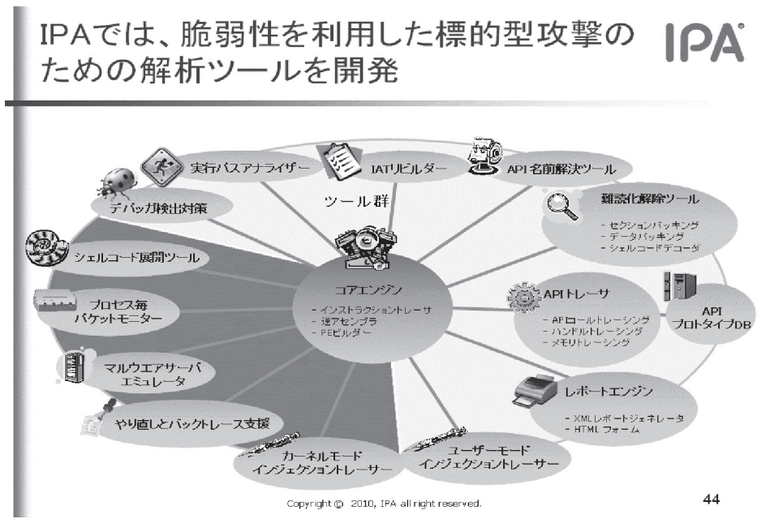


図6.14　IPAの開発ツール

1) 標的型攻撃解析ツールの貸出
※貸出には、利用許諾条件合意書への同意が必要。
申し込み ・ 貸出に関する問合せ ： vuln-inq@ipa.go.jp（ガイド裏表紙掲載）
～貸出までの手順～
①IPAから、メールアドレスに確認メール送付。
②確認メールに返信する。
③利用条件合意書がメールで送られてくるので以下を記入しIPAに郵送。
・利用者 ・ ・ ・ 氏名 ・ 所属組織名 ・ 連絡先 ・ 印鑑
・利用者の直属の管理職（課長以上）・ ・ ・ 氏名 ・ 役職 ・ 印鑑
④ツールが郵送される。
⑤利用期限は1年で、更新の際は再度合意書を提出。

2) 開発者向け脆弱性 実習ツールAppGoat（2011年1月 公開予定）。
ウェブサイト運営者やソフトウェア製品の開発者が脆弱性対策の必要性及び対策手法等を演習環境で体験的かつ実践的に学ぶツール「開発者向け脆弱性実習ツール(AppGoat ： 仮称)」を開発 ・ 公開する。
利用申し込みに関する問合せ ： vuln-inq@ipa.go.jp

3) IPAではセキュリティに関する各種ツールの開発を計画し進めており計画の概要を次に示す。（**図6.15 ～ 6.17**参照）

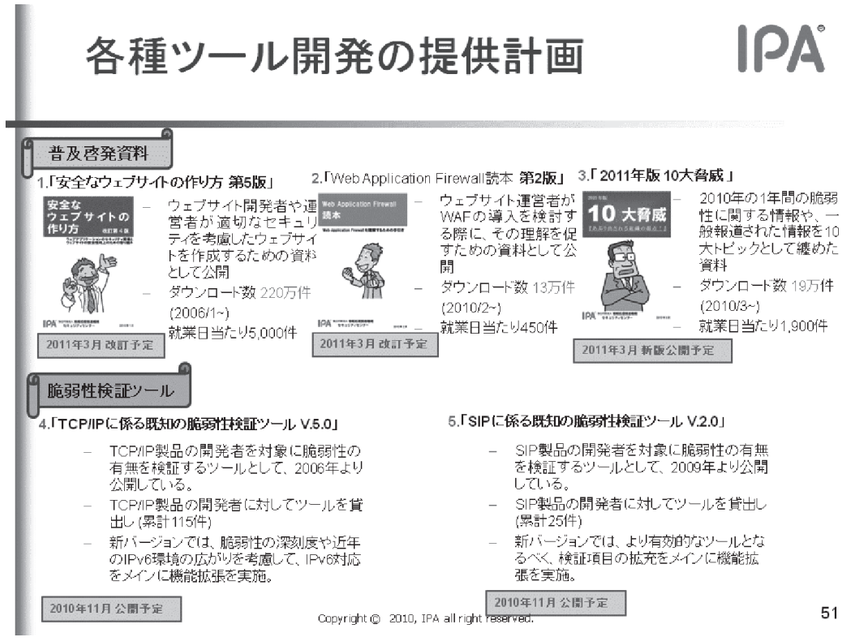


図6.15　各種ツール開発の提供計画(1)

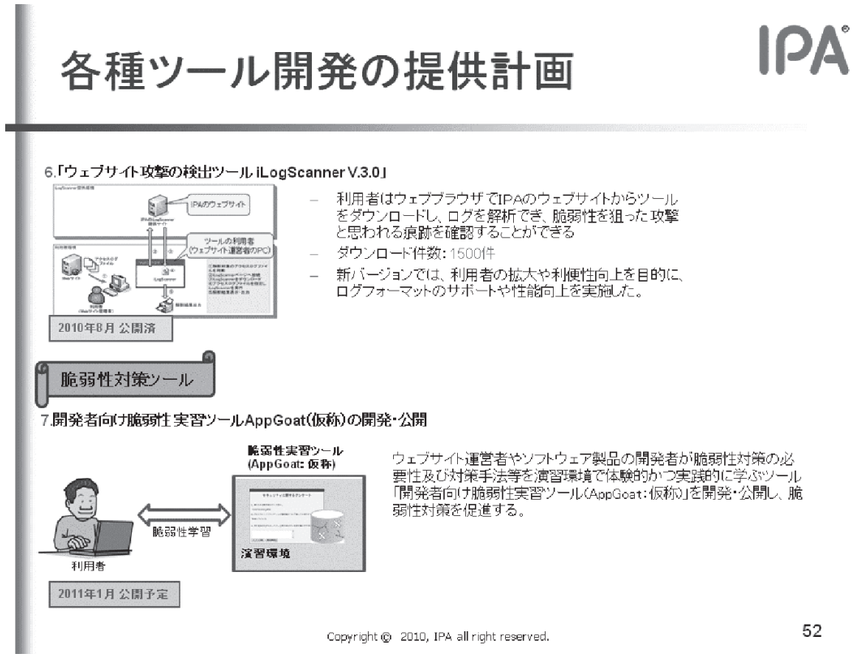


図6.16　各種ツール開発の提供計画(2)

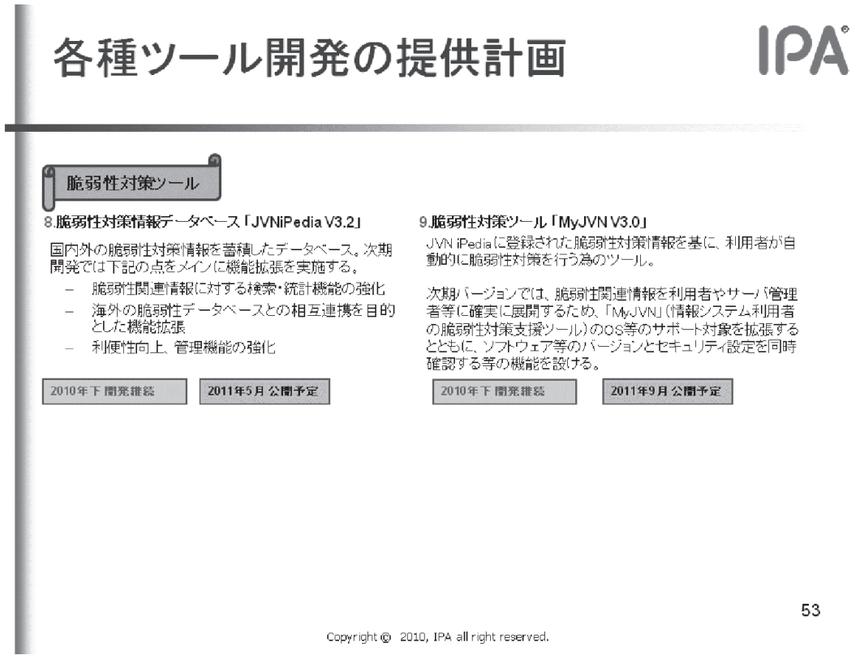


図6.17　各種ツール開発の提供計画(3)

6.3　組込みシステムのセキュリティへの取組みガイド

本節は、IPA情報セキュリティ技術ラボラトリーの萱島　信氏のご協力を得て、レポートにまとめたものである。

6.3.1　背景

2006年から3年間文部科学省の「科学技術振興調整費」を使って、組込みセキュリティ関係の研究を行っており、その3年間の成果として、セキュリティ上の課題を整理した「組込みシステムのセキュリティへの取り組みガイド」を公開した。その背景として以下の3点がある。

(1) 経済産業省の「2008年度組込ソフトウェア産業実態調査」では、組込システムは日本では重要な産業の位置づけにある(関連企業従事者数475万人で、全産業比率8.1%、製造業比率47.9%)。

(2) 総務省「平成20年度通信利用動向調査」によれば、日本での組込みシステムを取り巻く状況は年々普及率が上がっており、総務省「平成20年度通信利用動向調査」によれば、2008年度で携帯電話2.8%、カーナビ1.6%、ゲーム機1.6%、TV1.5%、家電1.0%などである。

(3) ネットワークに接続される製品が増え、機能・サービスが向上するなど著しく変わってきている。

6.3.2　組込みシステムのセキュリティの必要性

なぜ今組込みシステムのセキュリティが必要か？以下の4点が挙げられる。

(1) 組込みシステムがネットワークに繋がったことにより、ネットワークの脅威にさらされることになったこと、エンドユーザーの手に直接渡り、管理者が見てくれる訳ではない。

(2) 歴史が浅いせいか、組込みシステムには、アンチウィルスやファイアウォール等十分な対策がなされないまま利用されている。

一方で開発者の声として、

(3) コスト優先の現状では、セキュリティにリソースを割けない上に、一度事故が起こるとソフトアップデートが難しいし、多大のコストを背負う（訴訟費用を含めて）ことになり、IT系システムに比して切実である、

(4) 開発現場では手が廻らず、開発者のセキュリティ教育を実施するのも困難。

6.3.3　組込みシステムに特有な課題

PCなどIT系は、2000年に官公庁のHPが改竄された際の対策などある程度経験の積み重ねがあるが、組込みシステムにはまだそういった経験が少ない。また、組込みに特有な問題として以下の点がある。

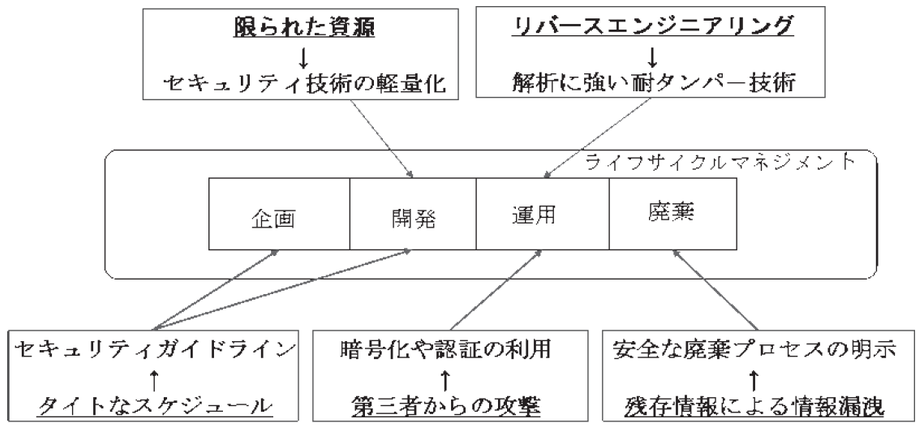
(1) 対策に製品回収が必要になる可能性がある（ハードとソフトが一体化されているため、修正パッチのみで対応できない可能性があるので、多大なコストを背負うケースもある。交換に120億円かかった事例も）。

(2) PCに比べ、多種多様な機能をもるため、人体に被害が及ぶ可能性がある（エアコンの設定温度の制御やカーナビ情報など、組込みシステムは人間が快適に生活するためのものや人命を預かるものもある。）そのため、セキュリティ上の弱点を突かれると、深刻な事故が起こる可能性がある。

(3) PCの事故は情報漏洩や金銭にまつわるものが大半だが、組込みシステムではそれだけではなく、人体に被害が及ぶ可能性が高い。例えば、エアコンの設定温度やカーナビのルート変更などである。ソフトとの関係を含めて機能安全の面がある。

6.3.4　製品に対するセキュリティ対策の基本

トータルな観点からの対策が必要との考え方から、**図6.18**に示すように組込みシステムのライフサイクルマネジメントである企画→開発→運用→廃棄のライフサイクル全体での対策が必要である。ライフサイクルをトータルで見ると、プロセスそれぞれの脅威に対する対策が重要となってくる。



下線：脅威，ゴシック：対策

図6.18　製品のライフサイクル

6.3.5　セキュリティへの取組みアプローチ

セキュリティ上の問題により、被害や損失が発生する以前に先ずは組込みシステムのセキュリティを意識することが必要で、セキュリティへのアプローチで目指したのは、以下の点である。

(1) 組込みシステムの開発に係わる経営者・開発者を対象に、セキュアな組込みシステムの開発を行なうために、ライフサイクル全体で取り組むべき指針を示す。

(2) 自組織へのセキュリティへの取組みレベルを把握できるように、ライフサイクルにおけるセキュリティ項目を16項目に分け、**表6.1**のように、それぞれの項目に対応した4つのレベルを策定する。

(3) 経営者、開発者に自組織のセキュリティに関する指針を示すことによって、セキュリティ意識の向上を目指す。マネジメントは、運用面のほか教育面、情報の収集体制を含む。

表6.1　セキュリティの取組みレベル

レベル	マネジメント方針	企画方針	開発方針	運用方針	廃棄方針
レベル 4	セキュリティへの組織的な取組みに加え、監査プロセスを有する	組織の方針に基づき、客観的評価を想定したセキュリティルールが策定および運用される		組織の方針として、脆弱性対策方針を定める共に、一般への公開を行う	客観的な基準に基づいたセキュリティリスクの軽減方法が用意される
レベル 3	セキュリティへの組織的な取組み（方針策定、実施）をしている	組織の方針に基づいてセキュリティルールが策定および運用される		組織の方針として、脆弱性対策方針を定めている	廃棄時のセキュリティリスクの軽減方法が用意される
レベル 2	セキュリティへの認識があるが、開発責任者や開発者の個人的な活動に限定される	セキュリティルールが開発責任者や開発者主導で策定および運用される		脆弱性対策方針を製品ごとに定めている	廃棄方法が仕様書等に明記される
レベル 1	セキュリティへの取組みを行っていない	セキュリティルールが開発責任者や開発者主導で策定および運用される		脆弱性に対する保証基準を設けていない	廃棄方法が考慮されていない

各レベルの説明：レベル1は、セキュリティへの取り組みができていないレベルで、ルール的なものが全くないが、レベル2はセキュリティの認識はあるものの、それが個人的な活動に限定されている場合である。レベル3になって、組織的な取組みがなされているレベルで、レベル4はセキュリティ監査など検証が行われているレベルである。

6.3.6　セキュリティを考慮すべき16項目

以下の**表6.2**に示す。

表6.2　セキュリティを考慮すべき16項目

ライフサイクル	説　明	項　目
マネジメント	セキュリティ商品ではなくても、メーカとして常に行うべき事項	①セキュリティルール、②セキュリティ教育、③セキュリティ情報の収集
企画・開発	ライフサイクル全体の計画およびシステムの開発を行なうフェーズ	④予算、⑤開発プラットフォームの選定、⑥設計、⑦ソフトウェア実装、⑧開発の外部委託における取組み、⑨セキュリティ評価テスト・デバッグ、⑩ユーザーガイド、⑪工場生産管理、⑫新技術への対応
運用	組込みシステムがユーザーの手に渡った後、製品として利用されるフェーズ	⑬キュリティ上の問題への対応、⑭ユーザーへの通知方法と対策方法、⑮脆弱性関連情報の活用
廃棄	買い替え、故障などで組込みシステムが廃棄、リサイクルされるフェーズ	⑯機器廃棄方法の周知

6.3.7　16項目の取り組みの説明

ガイドラインの初版は、2009年度セキュリティ項目15で作成したが、2010年はIPv6、Webインターフェース、GUIベースのブラウザ等の「新技術への対応」を拡充して16項目とした。

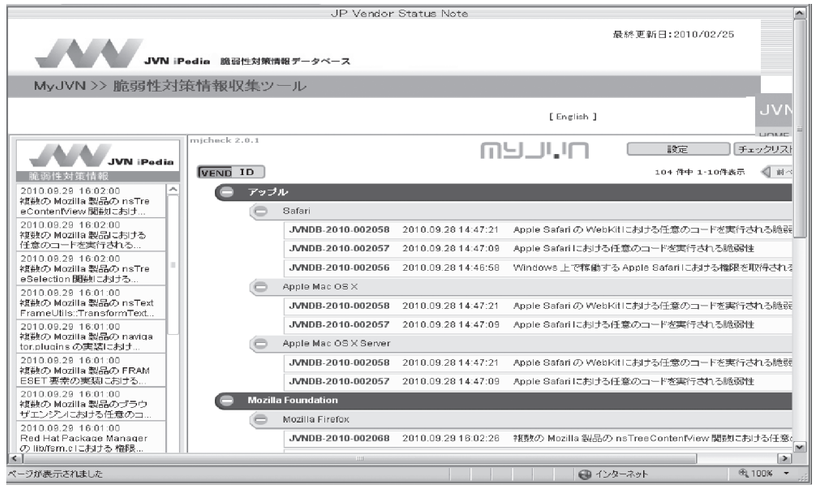
(1) マネジメント

①セキュリティルール ： 目的は取組みを場当たり的にしないための、実施すべき項目または禁止項目を明確にすることで、組織の取組みとしてはISMSが参考になる。これは、企業活動上機密情報を保護するためのISMSの規則類で、①情報セキュリティ基本方針 、②組織全体に関する情報セキュリティ管理規則 、③人的リソースに関する規則 、④開発体制 ・ 環境に関する規則 、⑤設計に関する規則 、⑥調達に関する規則 、⑦運用に関する規則 、⑧廃棄品として回収した機器に関する規則 である。

②セキュリティ教育 ： 脆弱性を作り込まないためには、現時点で知られている脆弱性に関する知識―例えば、①セキュア ・ プログラミングに関する知識 、②セキュリティテストに関する知識 、③情報セキュリティに関する知識―が必要である。ただし、セキュリティ教育は個人や一部のグループの自主的な活動にまかせるのではなく、組織としての教育システムをつくることが理想的である。また、Java、WindowsやUnixなどのEnterprise系がかつて持っていた脆弱性（ActiveXの脆弱性など）について組込み系に作り込まないように学ぶ体制作りも重要である。

③セキュリティ情報の収集 ： オープンソースソフトウェアは、開発元による積極的なセキュリティ情報の開示がないので、情報を取りにいく習慣をつける必要がある。セキュリティ情報の収集のための参照先としては、脆弱性に関する情報については、IPAのWebサイト（JVN iPedia、MyJVN）や暗号技術（2010年問題 ・ 規格動向など）に関してはCRYPTRECのWebサイトが情報を出しているので、効率的な収集ができる。

JVN iPedia



MyJVD

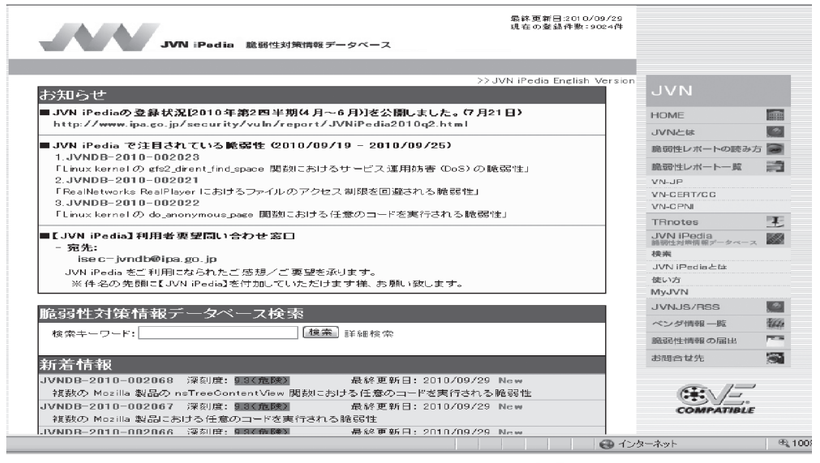


図6.19　JVNiPedia & MyJVDの画面

（2）企画・開発段階

④予算：セキュリティの問題は事前予測が困難だが、リスク回避の観点から、組込みシステムのライフサイクル全てのフェーズにおいて、全社的かつ継続的なセキュリティ予算を確保することが必要。さらには、有事の時ではないとお金は出しにくいが、プロジェクトリーダから要求があった場合に限り予算確保が容認されるのではなく、全社的に開発プロセスの一つとしてプロジェクト毎にセキュリティ予算が割り振られていたり、組織にセキュリティ部門を設置することが望ましい。

⑤開発プラットフォーム選定：大きくハードとソフトの2つがある。ハード（基板）の場合、「もの」がユーザーの手に渡るので、簡単にリバースエンジニアリングが出来てしまう。開発環境の選定に当たっては、ハードウェアは基板のデータバス上に機密情報が流れる場合、攻撃者による読み取りを困難なものを選定し、Webサーバに実際に流れる情報からリバースエンジニアリングが簡単にできるのを防ぐようにする。例えば、機密情報を扱うチップは端子からプローブされないものを選ぶとか、デバッグ用のピンを残さないよう配慮するとか、BGAようにチップの足が直接見えないものを選ぶとかする。ソフト（ファームウェア）の選定では、組込みソフトウェアパッケージを導入する場合には販売元の脆弱性対策に関するサポート状況を（何もしてくれないことを含め）事前確認すること。 Unixなどは、出来るだけカーネルバージョンは全社で統一を図る。

⑥設計：該当の組込みシステムのセキュリティ要件はISO 15408(CC)より抽出し、各セキュリティ要件に対しどのような対策を実施するかを検証すると良いが、コストがかかるので、セキュリティ要件をいくつかピックアップしておいた。セキュリティ要件例としては、機密情報の保護、障害復旧、サービス機能の保護、サイドチャネルアタック（信号の変化を攻撃する）、ハードウェアへの直接的な攻撃の対策、踏み台攻撃（某社のDVDのインターネットからの予約機能の脆弱性）への対策（認証）、付加機能として、アラート機能/ロギング機能/廃棄機能の付加などが挙げられる。設計段階のセキュリティ対策は開発担当者に一任されているのではなく、チェックリストを作るなど組織として設計段階で行うべきルールを規定すべきである。

⑦ソフトウェア実装：攻撃者のソフトウェア自身の振る舞いを解析する可能性に対しては、ソフトウェアの追跡が出来にくくするための技術であるソフトウェア耐タンパ性の確保が有効である。暗号モジュールなどで行われていることがあるが、やりすぎるとデバッグが大変なので、注意が必要である。インジェクション攻撃など、攻撃者が想定外のデータをソフトウェアに送り込んで誤動作を引き起こさせる可能性に対しては、セキュア・コーディングとツールを用いたソースコードレビューの実施で対処する（例えば、バッファオーバフローなどはスタックオーバフローを起こす長いデータをチェックするライブラリを使っていれば起きな

い）。

⑧開発の外部委託における取組み：組込みシステムの大規模化と開発コストの増加を抑制するため、システムの一部を外部（海外へも）委託するケースが増加しているが、セキュリティ上委託先に自社とまったく同じ取組みを求めることは困難である。そこで以下の対策をとる。→①セキュリティルールを策定して委託することが重要②特にプラットフォームになるような土台部分の設計を委託する場合、設計ルールや選定基準を明示③セキュリティルールの取組みが行われていることを確認する手段を設ける④セキュリティ対策に関連する検収条件を設定⑤委託先とのコミュニケーションを密にし、実態に即したセキュリティルールの運用に配慮する⑥問題発生時の責任範囲を契約上で明確化する（最終的にコスト負担になる）ことが重要である。

⑨セキュリティ評価テスト・デバッグ：以下の組み込みシステムに対する代表的な攻撃の対策が行われているか検証すること。①インジェクション攻撃 ②フォーマット攻撃③バッファオーバフロー④DoS攻撃（→ 以上セキュアプログラミングの観点からソースをチェック）⑤リバースエンジニアリング⑥サービス用ポート等の悪用⑦サイドチャネル攻撃（→ 以上製品の中味のハードウェア的な防護が行われているかチェック）

⑩ユーザーガイド：脆弱性は運用フェーズに入ってからも発見されるので、それを念頭に、対策に必要な情報、例えば、システムをセキュアに使用するためのユーザーガイド（→ パスワード設定の手段と、その手順を実施しなかった場合の問題についての説明など）に明記しておくものとして、①トラブル対応手順（→ セキュリティ問題が起きたときの対処法（電源オフ、リブートなど）②法的な免責事項③対応しているセキュリティ規格（→ 暗号、認証等で採用したセキュリティ規格名を明記）などはユーザーガイドに明記すべきである。これらは、機能安全と同じこと。

⑪工場生産管理：組込みシステムは、多くの場合工場（海外を含む）で組立てを行う際にソフトウェアの書き込みを実施するので、組立て工程において、情報漏えいやウィルス混入を発生させないための管理が必要となる。例えば個人情報や機密情報を扱うような場所には、何らかの障壁を設けることが望ましい。具体的には、物理的・ネットワーク障壁、ログ管理、物品管理、中間生成物の管理・廃棄などが考えられる。

⑫新技術への対応：今回の改訂で追加した目玉。IPv6やWeb技術などの新技術が取り入れられつつあり、それに応じたセキュリティに対する備えも必要である。例えば、IPv6ではグローバルなIPアドレスに対する保護（→IPv4では家庭内端末はNAT機能を使って外から見えないようにしているが、IPv6はグローバルアドレスが割り振られるので、P2Pのアプリケーションが作り易い半面、攻撃に直接さらされ

る可能性がある）やIPv6に特有のアドレス付与方式につけこむ攻撃の対策（→IPv6では、プールアドレスを複数ユーザーで利用するのではなく、組織のプレフィックスとユーザーの使用している機器のMACアドレスからIPアドレスを生成するため、ユーザーが判別可能になり、ユーザー情報が漏れる可能性がある）がある。Web技術では、内蔵Webサーバを用いた設定インターフェース（→ 攻撃者による各種インジェクション攻撃の対策）やブラウザ内蔵組込み機器（→ 接続先URLの表示、ポップアップ抑止、SSL2.0などの脆弱な暗号の利用抑止 ）など攻撃者に直接さらされる設計上の問題の阻止がある。

（3）運用段階

⑬**セキュリティ上の問題への対応** ： 組込みシステムの大規模化と開発コストの増加を抑制するため、システムの一部を外部（海外へも）委託するケースが増加しているが、セキュリティ上委託先に自社とまったく同じ取組みを求めることは困難である。そこで以下の対策をとる。→①セキュリティルールを策定して委託することが重要②特にプラットフォームになるような土台部分の設計を委託する場合、設計ルールや選定基準を明示③セキュリティルールの取組みが行われていることを確認する手段を設ける④セキュリティ対策に関連する検収条件を設定⑤委託先とのコミュニケーションを密にし、実態に即したセキュリティルールの運用に配慮する⑥問題発生時の責任範囲を契約上で明確化する（最終的にコスト負担になる）ことが重要である。

⑭**ユーザーへの通知方法と対策方法** ： 脆弱性が発見された場合、脆弱性の程度に応じて、修正プログラムやアップデートの適用 ・ 回収 ・ 修理が必要になる。そこで、ユーザーに通知する方法としては、郵送（はがき）、電子メール（スパムと誤認される可能性がある）、自社のWebページ、新聞の社告、脆弱性対策情報データベース（JVN）などの複数の方策がある。製品の特性を踏まえて、より確実にユーザーのもとに届くような様々な手法で通知を行う必要がある。

⑮**脆弱性関連情報の活用** ： セキュリティ問題を絶対に起こさせないようにすることは不可能（開発費とのトレードオフの問題などあり、非現実的）。脆弱性関連情報の活用で自社および製品のブランド価値毀損を防止するため、類似する他社製品での事例より、自社製品の問題を早期に把握し、自社での過去事例の対応を教訓とし、次の事故に備える。こうした対応策が回っていて常にブラッシュアップすることが必要である。

（4）廃棄段階

⑯**機器廃棄方法の周知** ： 組込み機器は、ユーザーが使用することによって個人情報などの機密情報がどんどん蓄積されていくので、廃棄された組込み機器から個人情報等が漏えいしないための仕組みが必要である。機密情報を守るためには、ユーザーが組込み機器を手放す際に簡単にこれらの機密情報を消去できるようにすることが必要（特にハードディスクなど全セクタに渡ってNullクリアしておく）。米国のNISTなど軍用では残存磁気により元のデータを推察される可能性があるため、消去のためのアルゴリズムが定義されており、ファイルを上書きするためツールなどもある。また、必要に応じて、製品の回収 ・ 廃棄には組織的に対応し、活動のための投資を行う必要がある。

6.3.8　16項目に対する取組みのレベル

組込みシステムメーカがセキュリティに取組むために、セキュリティへの意識、組織内のセキュリティルールの有無、組織の体制などを基準に1～4にレベル分けした。

- レベル１ ： セキュリティ対策は行われていない
- レベル２ ： セキュリティ対策は担当者主導のもと行われる
- レベル３ ： 組織としてセキュリティ対策に取り組んでいる
- レベル４ ： 組織としてセキュリティに取り組み、外部からの監査システムがある

内容の説明には、白物家電を作っているような人たちにも分かるように、少しずつ修正をかけている。

各レベルの詳細はガイドラインの巻末にあるA3サイズの資料にある。

6.3.9　本アプローチの活用法

本アプローチを活用するには，以下の3点がある。

(1) 自組織の把握 ： 自組織の「セキュリティへの取組み」と、本アプローチで定義したレベルとを見比べ、現在の自組織のレベルを把握する。

(2) より上位を目指す ： 今自分がいるレベルから、さらに上位のレベルを目指す。ガイドラインとしては、上位のレベルになるほど、より組織的にセキュリティに取組んでいることになる。

(3) よりセキュアな製品 ： 組織の「セキュリティへの取組み」のレベルが上がることで、その組織の製品の組込みシステムのセキュリティのレベルも上がり、よりセキュアな製品の実装が可能になる。

2009年6月に「組込みシステムセキュリティへの取組み」を出してから、2010年9月に改訂版を出した。読み物的なコーヒーブレークも追加したので、更に充実を図りたい。

6.3.10　今後の方向性

この成果をさらに多くの方に活用していただけるような取組みを行う。組込みシステムのベンダへのヒアリング等をもとに内容のブラッシュアップを図っていく。セキュリティ対策のためのツールや様々な事例を紹介するなど、組込みシステムのセキュリティレベル向上のための、より具体的な提案をしていく。今後も組込みシステムに関し、関係諸団体等と協力して、利用者やメーカー、サービス事業者のセキュリティ対策の向上に向けた活

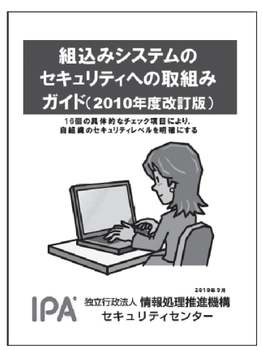
動を行ってゆくので、さらに具体的な提案などご協力をお願いする。

6.3.11　組込みセキュリティに関するIPA発行ドキュメント

時系列的に記載すると、**表6.3**のようになる。

表6.3　組込みセキュリティに関するIPA発行ドキュメント

ドキュメント名	発行日	対応する組込みシステムのライフサイクル
現場技術者向け「40のポイント集」 経営者向け「組込みセキュリティ資料」	2006/05/19	企画
組込みシステムを含んだソフトウェアの脆弱性関連情報の受付・蓄積・公開	2007/04/25	運用
組込みシステムの脅威と対策に関するセキュリティ技術マップの調査研究	2007/05/10	企画
セキュア・プログラミング講座	2007/09/25	開発
複数の組込み機器の組合せに関するセキュリティ調査研究	2008/01/29	企画
報告書（第4版）、検証ツール「TCP/IPに係る既知の脆弱性検証ツール」	2009/01/08	企画
報告書、検証ツール「SIPに係る既知の脆弱性検証ツール」	2009/04/23	企画
自動車と情報家電の組込みシステムのセキュリティに関する調査研究	2009/03/10	企画
組込みシステムセキュリティへの取り組み 組込みシステムセキュリティへの取り組みガイド（2010年度改訂版）	2009/06/24 2010/09/07 （改訂版）	運用
国内外の自動車の情報セキュリティ動向と意識向上策に関する調査研究	2010/04/15	開発



本成果はIPAの下記Webサイトでダウンロードすることができる。

http://www.ipa.go.jp/security/index.html

6.3.12　Q&A

(1) ガイドラインはレベル分けしているが、これから認定制度的なものへもっていけるか？

→セキュリティの格付けや認定制度的なものを作ろうとするとコストがかかり過ぎること、ISO/IEC 15408は多岐にわたっているので、専門家がいないと使いこなすのが難かしいこと、また、ジャンルを絞らないと、あるいは経済産業省のような権威ある組織を巻き込まないと実効的な認定基準は難しい。

(2) セキュア・プログラミング/コーディングについては、具体的には体系だったものか、経験的なものか？また、技法と言われるものはあるか？

→エンジニアリングとして体系だったものは未だない。ベカラズ集的に事例ベースに積み上がったものだったり、インジェクション攻撃では、入力データをサニタイジングするような後手後手に回ったTIPs集的な作りになる。ただ、入力データのサニタイジングやクレンジングなど技法に近いものもある。

(3) 4レベル定義されているが、セキュリティの場合定量的に管理できているか？また、外部監査はISMSやISO/IEC 15408の認証レベルを想定しているのか？

→運用面も入っているので、定量的な評価はできない。外部監査については、自組織でISMSやISO/IEC 15408的な基準を作ってチェックすることはできるが、両方とも触れていない部分、例えば納品後の運用面や廃棄についての認証基準は本ガイドラインが初めてとなる。レベルに対する監査サービスは無い。

(4) 自己宣言したレベルに対してIPAが承認を付与してくれるか？

→システム自体多岐に渡るので一般的には難しいが、家電のディジタルTVのように業界単位に限定すれば可能かと思われる。

＊＊＊　　第1部の執筆者一覧　　＊＊＊

第2部

組込みシステム業界における機能安全対策の調査研究

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

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（2010年）は、機能安全に関して何かと話題の多い年でした。年初にプリウスの暴走問題が米国でとりあげられ、ソフトウェアの危うさに話題が集まりました。結局、今年の2月8日に米運輸省と米航空宇宙局（NASA）が8ヶ月に及ぶ調査結果を発表し、電子制御機器に欠陥は認められなかったと発表し、収束の兆しを見せています。この問題は、多くの論点を提起していますが、ソフトウェアの安全性に関心が高まったことは確かです。

そして、2010年4月30日には、IEC 61508 Ed.2（機能安全規格改訂版）が発行され、JIS C 0508 の改訂作業がスタートしました。自動車の安全規格 ISO 26262 も大詰めを向え、2011年の夏には発行されるだろうとの見通しです。

このような流れの中で、本ワーキングは、昨年に引き続きいろいろな安全へのアプローチ例の調査を続けてきました。また、これまでの調査・研究の成果をまとめて、2010年7月に安全設計入門書も出版しました。12月のET2010では、3時間セミナーも企画し啓発活動も実施し好評を得ました。本報告書は、これら一年の活動成果を記載しました。

第1章は、機能安全規格IEC 61508の改訂版概要、ISO 26262の課題と認証対策、セーフウェアについて、調査結果をまとめています。また機能安全の先行事例として、宇宙（前年度実施したものですが、紙面の関係で本年度報告に編入）・医療・ドイツ産業界の例を調査しまとめました。

第2章は、2010年11月から2011年1月にかけて、ネットを使った調査と東京開催の展示会を調査し、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。これは一昨年から継続している活動で、3回目となります。安全設計をゼロから始めるのはたいへんですが、これら既存製品を活用することで、安全対応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ないことはご承知おき下さい。

第3章は、昨年から開始した用語集編纂です。今年は、IEC 61508Ed.2とISO 26262 DISもサーベイして、用語を追加しました。ただし、JISの改訂がまだであるので、用語の和訳は、見送りました。

過去の報告書とあわせ、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。

JASA　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2部）

第１章
安全性向上に関する活動の事例調査

近年、多くの製品にマイコンが組み込まれ、その故障や不具合においては、思いがけない危険を人に及ぼしかねない。製品を設計するときには、人間に危害を及ぼすような危険源とならない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完全な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の構築によって、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求められ、組込みシステムにおける安全性も議論されることが増えてきた。

そこで昨年度から実施している事例調査の一環として、第１章では、2010年4月に制定されたIEC 61508第2版、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、医療、航空宇宙といった各分野の機能安全事例について紹介する。また、機能安全規格の推奨する設計・検証手法（含む形式手法）に関する紹介、欧州での機能安全とは異なる米国発のシステム安全へのアプローチとしての「セーフウェア」などについても紹介する。

1.1では、機能安全の新たな展開としてIEC 61508第2版の概要について東京海洋大学佐藤教授のご見解を基に紹介する。

1.2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㈱の事例を基に紹介する。

1.3では、医療電気機器の安全試験実務と規格制定の裏話について（地独）東京都立産業技術研究センターの製品化事例を基に紹介する。

1.4では、安全への取り組みと日本への導入事例についてシーメンス㈱の事例を基に紹介する。

1.5では、セーフウェア（安全・安心なシステムとソフトウェアを目指して）の概要について翻訳された内容及び、㈱日本機能安全の事例を基に紹介する。

1.6では、安全に寄与するための分析、設計、検証（含む形式手法）について名古屋市工業試験研究所の取組事例を基に紹介する。

1.7では、航空宇宙の安全について（独）JAXAの事例を基に紹介する。

1.8では、機能安全に関する認証製品についてオムロン㈱の製品事例を基に紹介する。

1.9では、2010年12月1日に開催されたET2010において行ったJASA技術本部セミナーについて概要を紹介する。

1.1　機能安全の新たな展開(IEC 61508 改訂版の概要)

本節は、東京海洋大学佐藤吉信教授が平成22年4月27日のJASA/ETセミナーにて講演された内容を元にレポートをまとめたものである。

1.1.1　IEC 61508 制定状況

2009年12月にFDIS（Final Draft International Standard）が出版された。その賛否投票が2010年2月に終了し、第1部から第7部まで、FDISが全て承認された。そして、2010年4月30日にIS（International Standard）改訂第2版が発行された。改訂は、10年ぶりである。主な変更点を以下に記す。

1.1.2　全安全ライフサイクルの改訂

第５フェイズから、E/E/PEシステムの安全要求仕様が分離独立して第９フェイズとなった。そして、旧第９フェイズは、第１０フェイズにずれた。また、旧第１０フェイズのその他の技術を用いた安全関連系（の実現）と旧第１１フェイズの外的リスク軽減措置（の実現）とが統合されて第１１フェイズのその他のリスク軽減措置（の仕様と実現）となった。以上を図1.1.1に示す。また図1.1.2に全安全ライフサイクル改訂部分を示す。

1.1.3　用語定義に係る改訂（新設または追補）

（1）安全用語関連

a．危害事象

初版では、危険事象（hazardous event）のみであったが、今回危害事象（harmful event）が加わった。前者は、危害をもたらす可能性のある状態であるのに対し、後者は、危害（状態）の開始である。例えば複数の防護層を備えたプラントで、中間防護層の安全機能が失敗した場合は、危険事象が生起し、最終防護層の安全機能が失敗すると危害事象が生起するというような使い分けが可能となった。

b．目標リスク

全体システムにおけるある潜在危険による危害リスクに関して、その軽減又は緩和により達成すべき目標の水準。ＳＲＳ（安全関連系）は全体システムにおける現行の危害リスクを目標リスクまで軽減（低減）又は緩和しなければならない。こうして達成された安全を機能安全という。

（2）機器と装置に関する用語

a．環境

ＳＲＳ（安全関連系）がその全安全ライフサイクルの各フェイズにおいて関わる自然環境、運用環境、規制条件、保全条件など。

b．その他

「システムソフトウェア」、「既製のソフトウェア」、「ソフトウェアオンライン支援ツール」、「ソフトウェアオフライン支援ツール」、「ＡＳＩＣ（特別仕様集積回路）」などが追加。

（3）安全に係るシステム

a．その他のリスク軽減措置

現行の「その他の技術を用いた安全関連系」と「外的リスク軽減措置」とを統合してこの用語にした。

b．その他

「サブシステム(sub-system)」、「要素(element)」などが追加。

（4）安全機能と安全度に関して

a．全安全機能(overall safety function)

ある特定の危険事象に関して、被制御機器（ＥＵＣ）に係る安全状態を達成又は維持する措置。

b．要素安全機能(element safety function)

ある全安全機能を支援するために用いられる要素の機能。従来の安全機能が全安全機能と要素安全機能とに階層化された。

c．決定論的能力（systematic capability）

SIL １からSIL ４までの度合いで表す信頼（confidence）の尺度。ここで信頼とは、ある要素の決定論的安全度がこの要素に係る規格準拠アイテム安全手引書（1-8(1)参照）に定められた指示に従う使用条件下で、当該要素安全機能に関して当該SILの要求事項に適合するという確信である。

d．作動要求モード

現行では作動要求モードを２モードに分類しているが、「低頻度作動要求モード」、「高頻度作動要求モード」、「連続モード」の３モードに分類した。ただし、SILと作動要求モードの関係を示す表には変更はない。

e．目標機能失敗尺度

現行では「高頻度作動要／連続モード」に対して単位時間当たりの平均失敗確率と定義していたが、改訂版では「高頻度作動要求モード」及び「連続モード」に対して、単位時間当りの平均危険側故障頻度（すなわち故障強度）とした。

f．その他

「ＳＲＳ安全機能要求仕様」、「ＳＲＳ安全度要求仕様」などが追加。

（5）フォールト、故障、エラーに関して

a．故障（失敗）

現行では、ディペンダビリティ用語の故障の定義「機能ユニットが要求される機能を提供する能力を喪失すること」と同様であるが、改訂版では当該定義に「機能ユニットが要求されるものとは別の動作をすること」が追補された。

b．作動要求時危険側機能失敗確率（ＰＦＤ）

被制御機器（ＥＵＣ）又はＥＵＣ制御系から作動要求が発生した時の安全機能遂行に関するＳＲＳのアンアベィラビリティ。

c．単位時間当りの危険側故障確率（ＰＦＨ）

ＳＲＳが当該安全機能を遂行する所定の時間間隔におけるＳＲＳの危険側故障の平均頻度。

d．処置安全時間（process safety time）

ＥＵＣ又はＥＵＣ制御系に危険事象を引き起こす可能性のある故障が発生してから、当該危険事象が起きない様にＥＵＣの処置を完了するまでの許容時間。

e．その他

「安全側故障」、「ソフトエラー」、「無関係部位の故障」、「無影響故障」、「安全側故障割合（ＳＦＦ）」、「故障率」、「作動要求時の平均危険側故障確率（ＰＦＤavg）」、「平均修復時間（ＭＴＴＲ）」、「平均修復時間（ＭＲＴ）」などが追加。

（6）ライフサイクル業務に関して

a．コンフィギュレーションベースライン

ソフトウェアリリース（software release）が審査可能で系統的に改造できるようにするための情報。これは、次を含む：ソフトウェアリリースを構成する全てのソースコード、データ、ランタイムファイル、ドキュメンテーション、コンフィギュレーションファイル及びインストールスクリプト；ソフトウェアリリースを作成するために使用したコンパイラー、オペレィティングシステム及び開発ツールに関する情報。

（7）安全措置の確認に関して

a．規格準拠アイテム安全手引書（compliant item safety manual）

システムが IEC 61508 の要求事項に適合することを保証するために必要な要素について、当該要素安全機能に関して、当該要素の機能安全に係る全ての情報を提供する文書。

b．使用実績による証明（proven in use）

ある要素のある特定のコンフィギュレーションに関して、危険側決定論的フォールトの確からしさがその要素を使用するそれぞれの安全機能に必要とされる安全度水準を達成するのに十分な程に低いことの運用経験に基づく実証。

c．その他

評価者（アセッサー）などが追加。

1.1.4　規定内容の主要な変更点と問題点

機能安全は、多様な技術を包括する新しいパラダイムなので、第２版は、発行されたものの、未だ技術的に成熟していない分野である。そのため多くの問題が存在している。

以下の３項目は、次回改定への継続審議案件となっている。

（注 ： 詳しくは計装２０１０年１月号（Vol.53 No.1） ｐ９～ｐ１３を参照）

(1) 目標機能失敗尺度について

目標機能失敗尺度をＰＦＤavgとＰＦＨで規定している。（これは必ずしも適切な定量化モデルであるとは言えない。）

(2) 故障と危険（危害）事象について

改訂版では、“failure”を①信頼性工学で定義されるいわゆる「故障」、及び、②機能（運転）に失敗することとの二通りの意味で定義している。これは、本規格の理解を困難にしている大きな理由でもある。

(3) 危険事象生起モデルについて

危険（危害）事象が生起する場合、a）ＳＲＳがフォールトにある時（動作可能ではない時）に作動要求が発生する、ｂ）安全機能の実行が必要な作動要求状態にある時にＳＲＳが当該機能に失敗する、という二通りの場合が存在する。

改訂版では、ＰＦＤavg を安全関連系（ＳＲＳ）の安全機能に係るアンアベィラビリティで定義している。これは、ａ）のみを想定しており、ｂ）を想定していないことを意味する。危険事象率の計算で大きな誤差を伴うという報告もある。

(4) 選択肢　１ｓ、２ｓ、３ｓ

決定論的安全度（決定論的能力）に係る要求事項の実施では、次の選択肢 １ｓ、２ｓ、３ｓ のいずれかを選択することができるようになった。

[選択肢1s]

ハードウェア、ソフトウェア又はシステムの決定論的フォールトの回避に係る要求事項（第２部7.4.6項及び第３部）、及び、決定論的フォールトの制御に係る要求事項（第２部7.7節及び第３部）に準拠すること。

[選択肢2s]

当該機器（ハードウェア、又はソフトウェアを含むシステム）が「使用実績により証明済み（proven use)」である証拠に係る要求事項に準拠すること。（第２部7.4.10項)。

[選択肢3s（既製品のソフトウェア要素のみに適用)]

第3部7.4.2.12項に準拠すること。

選択肢が増えた理由は、使用実績のある要素に対して、新規の要素と同じ要求事項を課すことは現実的ではないという意見が改定会議で多かったためである。

(5) 選択肢　１Ｈ、２Ｈ とＳＦＦ（安全側故障割合）

ハードウェア安全度に係る構成上の制約事項として次の選択肢１Ｈ、選択肢２Ｈのいずれかを選択して準拠することになった。分野規格においては、どちらかの選択肢を指定することもできる。

[選択肢１Ｈ]

現行のハードウェアフォールトトレランスとＳＦＦによる制約事項。

[選択肢２Ｈ]

最終使用者のフィードバックによるコンポーネントの信頼性データと（選択肢１Ｈに比して）より高い信頼水準の信頼性（故障）データの使用、及び、それぞれの安全度水準に対するハードウェアフォールトトレランス規定による制約事項。

選択肢２Ｈが導入された理由または背景は以下である。

a．安全側故障の安全側は明確に定義できない場合がある（状況が変わると安全側が逆になる場合がある)。

b．ある潜在危険に係る安全側故障が増加すると、別の潜在危険による危険性を増大させる場合が存在する。すなわち、安全側故障の増加はいつもシステム全体を安全側にするとは限らない。

c．安全側故障を明確に定義できる場合、安全側故障は意図的に比較的容易に増加させることが可能である。例えば、半田付けの品質を落とすことにより、断線故障が増加し、これが安全側故障割合を高める。

d．安全側故障を明確に定義できる場合、安全側故障は意図的に比較的容易に増加させることが可能であるが、これにより低頻度作動要求モードにおいて若干（数パーセント）危険事象率を低下させるかもしれない。

これは、安全側故障により全体システムが安全トリップ発動させ、これが結果的にプルーフテストの役目を代替することになるためである。しかし、プルーフテストの回数を増加させた方が安全トリップを発動させ、これが結果的にプルーフテストの役目を代替することになるためである。しかしプルーフテストの回数を増加させた方が安全トリップを発動させるよりも遥かに経済損失は少ない。

e．ＳＦＦと故障データの信頼性との関係は、未だ技術的あるいは学術的に明確ではない。ＳＦＦは全故障率中の各種故障率の割合を規定している。全故障率が信頼できな

ければＳＦＦの値自体も信頼できない。

選択肢２Ｈは、１Ｈに比して意味を持つが、それだけに実施が遥かに困難な規定である。従って、多くは１Ｈが選択されるのではないかと予想される。

（6）規格準拠アイテム安全手引書

当該ＳＩＬを発揮可能とする使用条件を記したものが安全手引書であるが、以下の問題点を含んでいる。

- サブシステムや部品は、安全関連系の中でどのように使用されるかによって、すなわち、遂行する安全機能、作動要求モード、プルーフテストなどの条件が異なれば、全く異なるＳＩＬを持つことになる。
- あるサブシステムがある安全関連系に使用されるとＳＩＬ３にもなり、別の安全関連系に使用されるとＳＩＬ０かもしれない。
- 本来、サブシステムや部品は、使用される条件下でのＳＩＬを示さなければならない。

1．全安全ライフサイクルの改定

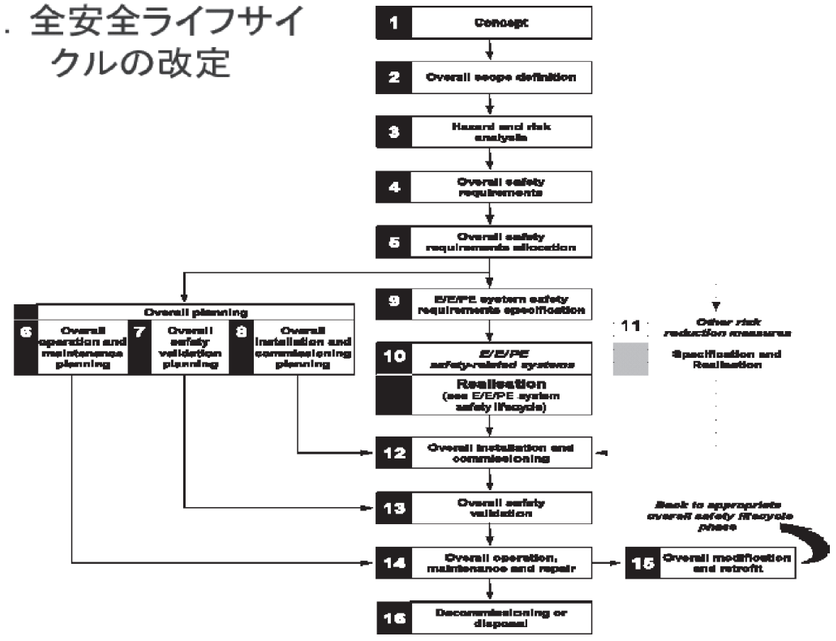


図1.1.1　旧全安全ライフサイクル

全安全ライフサイクル　(改訂部分）

安全度水準を満足する安全関連系を実現するための 道標として「全安全ライフサイクル」を規定し、リスク分析、設計から、運用、保守、廃棄に至るまでの 規範手順 を示している。

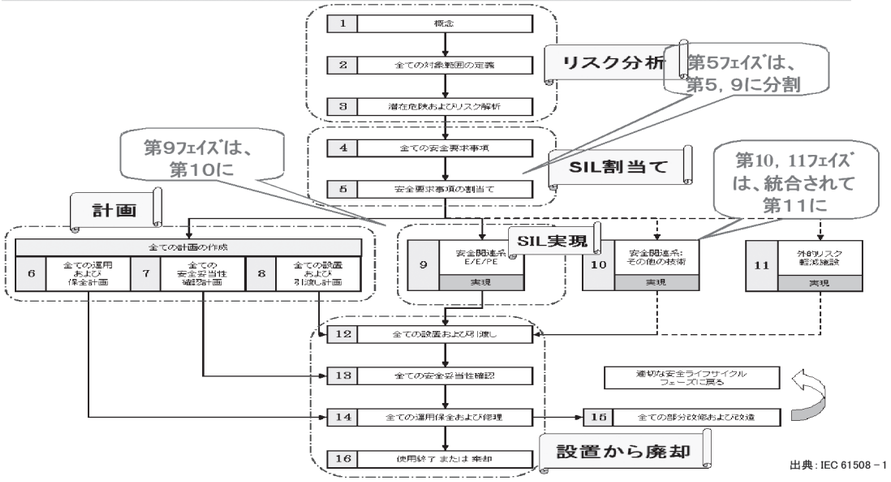


図1.1.2　全安全ライフサイクル改訂部分

1.2　ISO 26262対応の課題と認証対策について　（テュフズード社）

本節はテュフズードジャパン株式会社の御協力を得て、2010年4月27日に開催されたJASA/ETセミナーの竹市正彦氏の講演（ISO 26262対応の課題と認証対策について）をベースに当委員会がレポートをまとめたものである。

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「Tenchnischer Überwachungs Vevein」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ことになった。

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。

1.2.1　ISO 26262対応のポイント

自動車向けの安全規格であるISO 26262は2011年には正式に国際規格として発行される。

その内容は以下の構成で成っている。

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（ハードウエア）
第6部　製品開発（ソフトウエア）
第7部　生産・運用
第8部　支援プロセス
第9部　ASIL指向、安全指向の分析
第10部　ISO 26262のガイドライン

ここでは、テュフズードジャパンから見たISO 26262への対応を行う上でのポイントとして

（1）機能安全の管理（Management of Functional Safety)
（2）Core Process
（3）Tool/Support Process
（4）ASIL-oriented and safety-oriented analyses

について紹介する。

（1）機能安全の管理（Management of Functional Safety）

ISO 26262で記述されている機能安全の管理には以下のような項目がある。これらは、自動車産業向けの品質マネージメント規格である「ISO TS 16949」及び欧州の車載製品開発標準プロセスである「Automotive SPICE」の上に成り立つものである。

・総体的な安全管理
　－　安全文化
　－　プロジェクトや資源の管理
　－　安全ライフサークル-品質管理
・安全管理-アイテムの開発
　－　役割と責任
　－　安全管理

－　安全ライフサイクルのアプリケーション
－　安全状態
－　確認測定

・安全管理-製品発売後
－　ライフサイクルの確保、フィールドモニタリング

（2）Core Process

ISO 26262 におけるコアとなるプロセスには、ハザード解析及びリスク・アセスメントとソフトウェア開発モデルにおける設計フェーズ及びテストフェーズにおけるverificationプロセスと故障メトリックとして定義されるシングルポイント故障メトリック及び潜在的故障メトリックの評価、さらにsafety planの構築がポイントになる。

①ハザード解析及びリスク・アセスメント

ASIL（Automotive Safety Integrity Level）は運転稼動状況における先税危険の系統的評価に基づき決定している。重大度、危険度、危険にさらされる頻度、可能性も考慮している。これは、あらゆる安全機能においてＯＥＭとサプライヤー間で共有されているものである。

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

E/C/S⇒ASILの概要
A=ASIL A
B=ASIL B
C=ASIL C
D=ASIL D
C1=Controllability
E1～E3= Exposure
QM=Quality Management
S1～S3=Severity

図1.2.1　ハザード解析／リスク・アセスメント

②ソフトウェア開発モデルにおけるverificationプロセス

Design phase verificationで以前に設定した要求事項に合致していることを確認するための成果物評価とTest phase verificationでアイテムやそのパーツが要求する項目を満たしている事が確認できる。

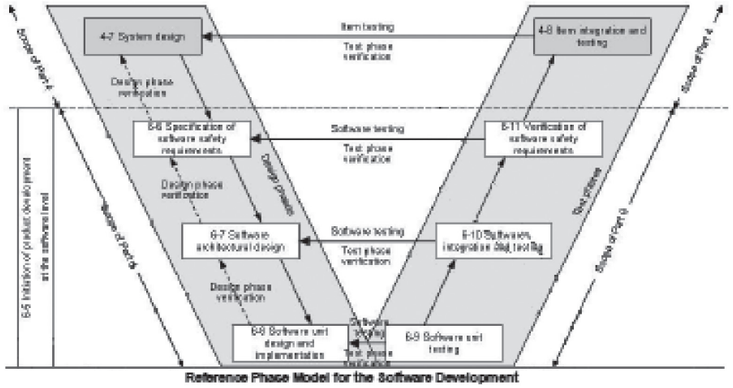
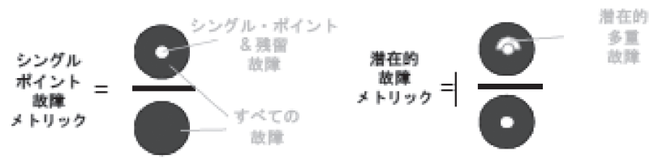


図1.2.2　Reference Phase for the Software Development

③シングル・ポイント故障メトリックと潜在的故障メトリック

システムにおけるASILを決定する要素としてコンポーネントに対するシングル・ポイント故障メトリックと潜在的故障メトリックによる評価がある。（**図1.2.3**参照）



	ASIL B	ASIL C	ASIL D
シングル・ポイント故障メトリック	＞90％	＞97％	＞99％
潜在的故障メトリック	＞60％	＞80％	＞90％

図1.2.3　Single point faults metric and latent faults metric target value

④safety plan

safety planは、safety caseに対してプロジェクトとして最初のステップとして考慮する必要がある。

開発計画として、プロジェクト計画、検証計画、品質保証計画、コンフィギュレーション管理計画を構築する。（**図1.2.4**参照）

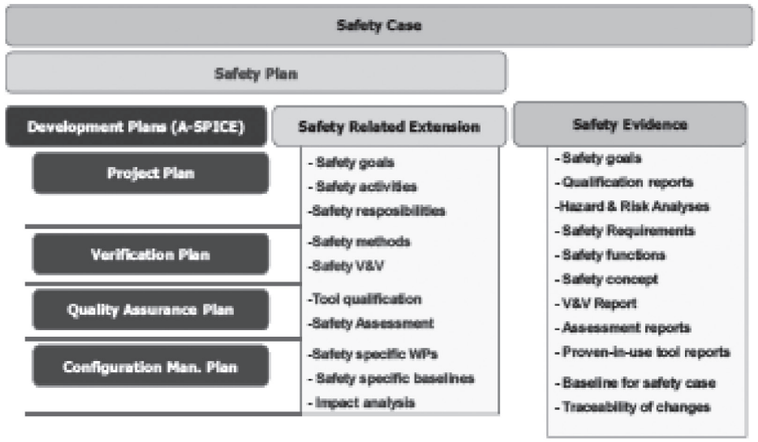


図1.2.4　Safety Plan

1.2.2　ISO 26262認証作業

ここでは、ISO 26262の認証作業における対策についてのポイントを紹介する。

（1）認証について

ー自動車の欧州認証システム

自動車/自動車部品の認証は必須です。

認証は

１）欧州の法規（Regulation, Directive他）に従って、

２）欧州で認められた試験機関（Technical Service）が試験、レポートを作成

３）各国の運輸省（Authority）が認可を発行します。

⇩

一般機械部品等の自己認証（CE-Marking）とまったく違います。

ー自動車認証における機能安全の要求について

１）現在車両認証システムの中で、以下の認証基準に機能安全の要求が盛り込まれています。

◆ブレーキ（ECE R13H）

◆ステアリング（ECE R79）

◆バッテリ式電気自動車（ECE R100）

２）今後、同様の要求が組み込まれると思われる認証基準

◆ESC（661・2009 General Safety Regulation）

◆Brake Assist System（78/2009 Pedestrian Protection Regulation）

例えばブレーキの車両認可を取得するためには、

①車両認証時通常のブレーキ性能試験レポートに合わせて機能安全評価レポートを当局に提出する必要があります。

②ブレーキシステムのサプライヤが、認知された試験機関の評価レポートを持っている場合は、車両メーカはそれ以外の部分のみ評価レポートを取得すれば済みます。

（2）TÜV　SÜD提供サービス（サービス　ポートフォリオ）

ここでは、テュフズードジャパンがサポートするサービスのポートフォリオを示します。

・安全電子装置の周辺の機能安全における自動車、ソフトウエア、半導体に関して以下のサービスを提供している。

ートレーニング

ーコンサルティング

ー分析論

ーアセスメント/証明書

①ISO 26262　機能安全の管理（Management of functional safety）

ここでは、機能安全の管理に対するＴＵＶによるサービスを紹介する。

ａ）機能安全プロセス管理に対するコンサルティングとアセスメントのためのアシスタント

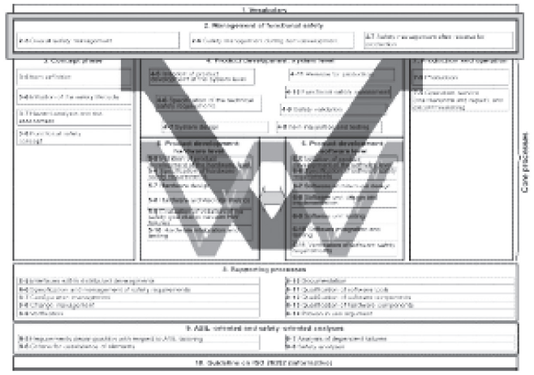


図1.2.5　Management of functional safety

a-1）要求されたwork productsに対するコンサルティングと判定

a-2）既存の開発プロセス、サポートプロセスから機能安全プロセスへの変換プロセスにおけるコンサルティングと判定

a-3）適用された安全測定に対するコンサルタントと判定

→　TÜVのアセスメントレポートはISO/DIS 26262の機能安全ためのクライアント管理に従って証明（またはギャップについて説明）する

b）コアプロセスのコンサルティングとアセスメントのためのアシスタント

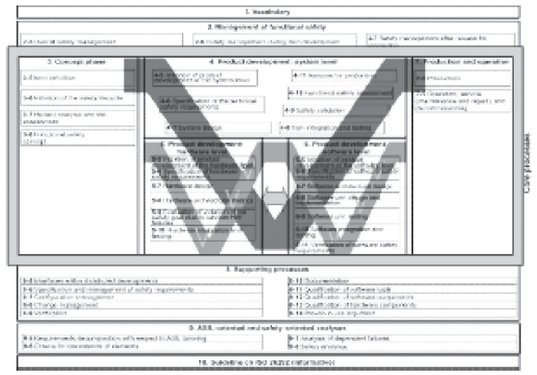


図1.2.6　Core process

b-1）プロセスとコンセプトフェーズで適用された方法に対するコンサルティングと判定

b-2）開発プロセスと適用された方法に対するコンサルティングと判定

◆システムレベル

◆ハードウエアレベル

◆ソフトウエアレベル

b-3）プロセスと製造と作成の適用された方法に対するコンサルティングと判定

b-4）要求されたwork productsのコンサルティングと判定

→　TÜVのアセスメントレポートはISO/DIS 26262の機能安全ためのクライアント管理に従って証明（またはギャップについて説明）する

c）支援プロセスのコンサルティングとアセスメントのためのアシスタント

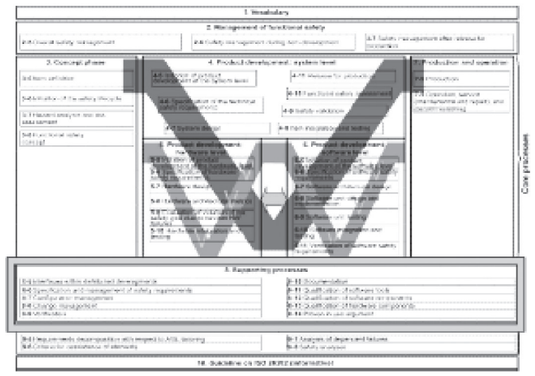


図1.2.7　Supporting processes

c-1）分散された開発におけるインタフェースのコンサルティングと判定

c-2）安全要求の管理と仕様のためのコンサルティングと判定

c-3）コンフィギュレーション管理のためのコンサルティングと判定

c-4）変更管理のためのコンサルティングと判定

c-5）検証のためのコンサルティングと判定

c-6）ドキュメンテーション管理におけるコンサルティグと判定

c-7）ソフトウエアツールの評価

c-8）ソフトウエアコンポーネントの評価

c-9）ハードウエアコンポーネントの評価

c-10）使用実績を立証された論拠への判定とコンサルティング

→　TÜVのアセスメントレポートはISO/DIS 26262の機能安全ためのクライアント管理に従って証明（またはギャップについて説明）する

d）ASIL-志向及び安全志向分析のコンサルティングとアセスメントのためのアシスタント

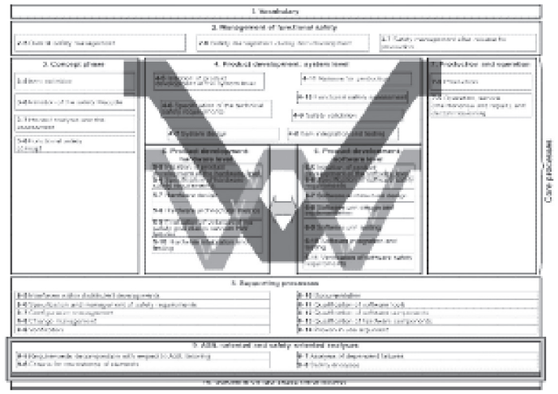


図1.2.8　ASIL-oriented and safety-oriented analyses

d-1）システム-ハードウエアとソフトウエアレベルにおける要求定義の分解のためのコンサルティングと判定

d-2）共通原因解析のコンサルティングと判定

d-3）安全解析（FMEA,FTA etc.）のコンサルティングと判定

→　TÜVのアセスメントレポートはISO/DIS 26262の機能安全ためのクライアント管理に従って証明（またはギャプについて説明）する

1.2.3　認証に関するまとめ

① ISO/DIS 26262の適用は確立された品質管理（ISO TS 16949/AutomotiveSPICE）プロセスの上にセットアップする

② ISO/DIS 26262は法的要求事項ではないが、自動車業界における機能的保証に関してテクノロジーの現在のスタンスを説明している

③ ISO/DIS 26262の導入は今後TUVから推奨される

④ 少なくとも2011年以降、サプライヤは自らの開発プロセスをISO 26262に従い説明することをもとめられる。

⑤ ISO/DIS 26262を導入するという意味はかなりの追加経費と明確なパイロットプロジェクトからはじめなくてはならない。

1.3　医療電気機器の安全試験実務と規格制定の裏話

本節は（地独）東京都立産業技術研究センター事業化支援本部技術経営支援室に所属されている岡野宏様の御協力を得て、レポートとしてまとめたものである。

1.3.1　（地独）東京都立産業技術研究センターの活動概要

大正10年に設立された府立東京商工奨励館（東京都立工業奨励館の前身）と大正13年に設立された東京市電気研究所（東京都電気研究所の前身）を始め4研究所が母体となる東京都立産業技術研究所と城東地域中小企業振興センター、城南地域中小企業振興センター、多摩中小企業振興センターの技術部門を統合するとともに、地方独立行政法人へ移行し、地方独立行政法人東京都立産業技術研究センターとなる。今回紹介する医療電気機器の安全試験実務を始めとする中小企業の事業ニーズに即した高品質な技術支援の実施により都内中小企業の振興を図り、これを通じて都民生活の向上に貢献するための活動を行っている。また、平成２３年度には臨海部に新たな本部拠点の開設を予定している。この本部拠点は、現在の北区西が丘の本部機能と世田谷区駒沢支所の機能を統合したもので、都内中小企業の目指す高付加価値ものづくりを支える活動を行っていく。

連絡先 ：

西が丘本部　東京都北区西が丘3-13-10

Tel ：　03-3909-2151

URL ；　http://www.iri-tokyo.jp/

1.3.2　医療機器の安全について

1.3.2では、医療機器の安全に関する考え方について最初に紹介する。医療機器の安全に関する基本的な思想としては、絶対に故障しない機器はありえないということが基となっている。基本的な医療機器製造・輸入承認の流れは、**図1.3.1**に示すように製品が実際に動作するかといった検査を含めて承認申請前に事前検査を行い、厚生労働省の承認を得て、医療機関に納入するというものである。医用電気機器における電気安全試験の根拠（**図1.3.2**）となる安全通則（薬事法）としては、以前は国際規格IEC 601-1（1988）であり、国内のJIS T 1001、1002（1992）であった。JIS T 1001、1002（1992）は、国際規格IEC 601-1（1988）の構成をJISの様式に合わせたことと、わかりやすくするために冗長な文章を簡略化したものである。これらのJISに規定されている内容は対応するIEC規格の内容でもあるのでIEC 601-1（1988）に適合するする機器はJIS T1001/T1002にも適合する機器と考えられる。また、本JISでは電源コード等においては現存するJIS規格品も使用できるように規定されている。

個別規格は優先度が高く、先ほどの通則よりも優先される。心電計は、JIS T

1202(1998)が、電気メスは、JIS T 1453(1998)が、低周波治療器は、JIS C 6310(1986)が優先される。

現在使用されている安全規格は、医用電気機器の安全性に関する一般的要求事項（**図1.3.3**）である。この規格は、JIS T 0601-1（1999）で、国際規格IEC 60601-1（1988）にAmendment 1（1993）とAmendment 2（1995）を加えたものであり、技術的内容を変更することなく、項番号、項タイトル等の構成も含めて日本語に翻訳された同一規格である。ただし、例えば、保護接地線を含む電源コードに既存のJIS規格品が使用できる、EMC対応については企業に一任といったように、国内事情を配慮して緩和された事項も含まれており、これらについては附属書に概説されている。従って、JIS T 0601-1に適合すればIEC 60601-1 に適合すると考えてよいことになる。

また**図1.3.3**では、システムという規格が含まれるようになった。システムというのは、医療機器と医療機器、医療機器と産業機器等を組み合わせたものを指す。

この国際規格の次バージョン第3版は既に存在するが、日本ではまだ翻訳中で発行されていない。第3版は何が新しくなったかと言うとリスクマネージメントまで含まれた点である。例えば、髭をそる場合に電気カミソリor安全カミソリor大型カミソリのどれを使うかといった際、使う人と使用する機器の大きさ等まで考慮しなければいけないことが含まれている。

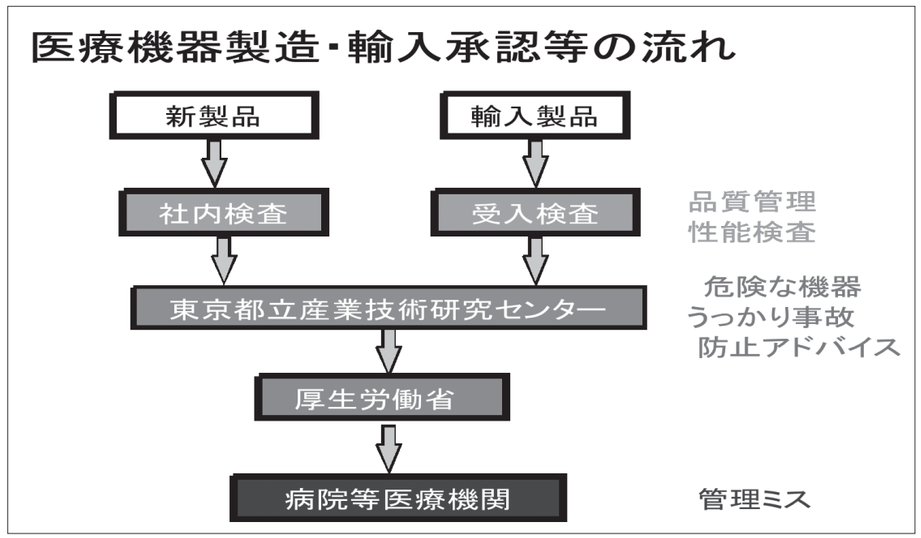


図1.3.1　医療機器製造 ・ 輸入承認等の流れ

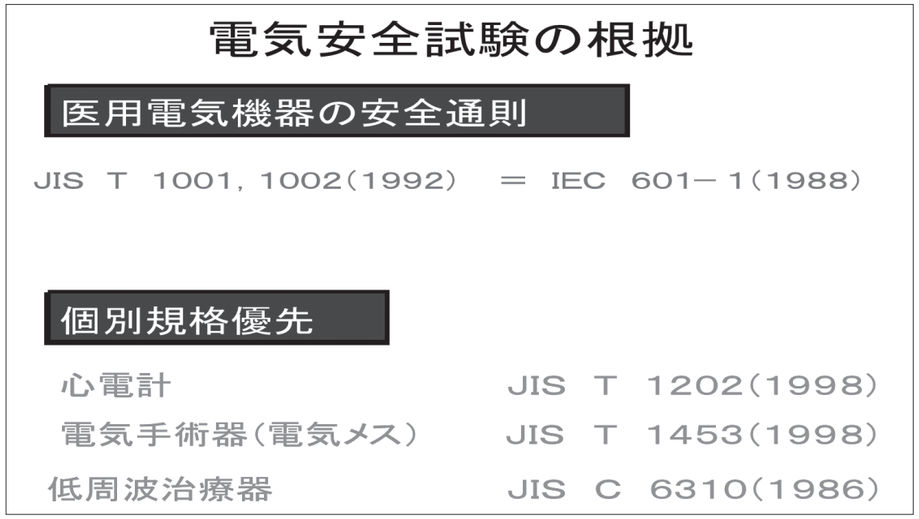


図1.3.2　医用電気機器における電気安全試験の根拠

図1.3.3　医用電気機器の安全性に関する一般的要求事項

図1.3.4に電撃による事故例を示す。人体に電流が流れるとショック症状や熱傷等が発生し、重度の場合は死に至ることがある。そのため、電気を使用する機器では、使用者に電流が流れないように安全を確保することが要求される。特に、患者さんを対象とする医用電気機器では、高い安全性が必要とされ、その安全規格としてJIS T 0601-1（1999）

が存在する。安全を確保するため、最初に機器内部の危険箇所を特定することが必要となる。JIS T 0601-1（1999）では、触れた場合に許容値を超える電流が流れる可能性がある部分と人体が接触する部分とを分離することが要求されている。電気的に分離する方法としては、絶縁する方法と保護接地する方法とがある。さらに、医用電気機器では高い安全性が求められることから、二つの手段を用いて分離することが要求されている。具体的には絶縁することによって分離した箇所をさらに保護接地する方法と絶縁を二重にして分離する方法とがある。

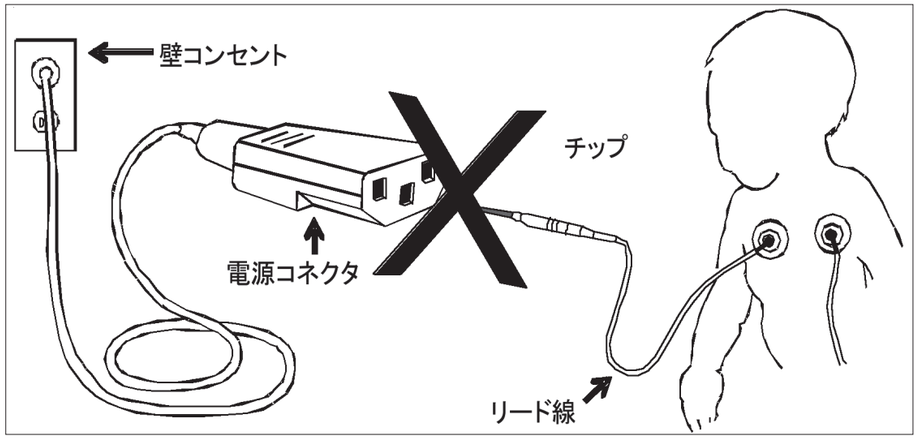


図1.3.4　医用電気機器の電撃による事故例

1.3.3　JIS化について

2005年から施行された薬事法改正によって、低リスク（クラスⅡ）の管理医療機器には、第三者認証制度が導入された。この、第三者機関が認証審査を行うための認証基準にJISが引用されることになり、理学療法機器分野で13のJIS化が行われた。

このJIS化に関与した立場から、作成上の問題点と対策について述べる。

まず、厚生労働省のクラス分類告示例（**図1.3.5**）について述べる。

①高度管理医療機器は、不具合が生じた場合、生命の危険に直結するおそれがあるもの、または、人体へのリスクが比較的高いと考えられるもので、801品目ある。

例 ： ペースメーカ、人工心臓弁、人工呼吸器、カテーテル等

②管理医療機器は、不具合が生じた場合でも、人体へのリスクが比較的低いと考えられるもので、1318品目ある。

例 ： X線診断装置、MRI、電子体温計、電子内視鏡、超音波診断装置等

③一般医療機器は、不具合が生じた場合でも、人体へのリスクが極めて低いと考えられるもので、967品目ある。

例 ： 電動式患者台、X線用テレビ装置、聴診器、血圧計等

厚生労働省クラス分類告示の例

	品目	機　器　例
①高度管理医療機器	801品目	★心臓カテーテル付検査装置 ★中心静脈カテーテル ★脳脊髄用ドレーンチューブ ★機械式人工心臓弁
②管理医療機器	1318品目	★X線心断検査装置 ★X線CT診断装置 ★MR装置 ★造影剤注入装置 ★電子体温計
③一般医療機器	967品目	★電動式患者台 ★X線用テレビ装置 ★聴診器　★血圧計 ★音叉　★握力計 ★コレステロール分析器 ★メス　★はさみ

図1.3.5　厚生労働省のクラス分類告示例

さらに厚生労働省の医療機器に係わるカテゴリ（**図1.3.6**）について述べる。

国際分類のクラスⅣ、Ⅲが高度管理医療機器に相当し、患者への侵襲性が高く、不具合が生じた場合、生命の危険に直結するおそれがあるもの、または不具合が生じた場合、人体へのリスクが比較的高いと考えられるものなので、機器の製造販売は、大臣による承認が必要となる。またクラスⅡが管理医療機器に相当し、不具合が生じた場合でも、人体へのリスクが比較的低いと考えられるものなので、機器の製造販売は、登録認証機関による承認または認証が必要となる。クラスⅠが一般医療機器に相当し、不具合が生じた場合でも、人体へのリスクが極めて低いと考えられるものなので、機器の製造販売は、承認・認証が不要となる。ただし、医療機器を製造販売する場合において、製造販売会社としての許可は受ける必要がある。

医療機器に係わる「カテゴリ」

薬事法上の分類	リスク	製造販売		販売許可	クラス分類
		許可	承認		
一般医療機器	極めて低い	○	×	×	クラスⅠ
管理医療機器	低い	○	承認又は【認証】が必要	【届出】が必要	クラスⅡ
高度管理医療機器	中・高	○	○	○	クラスⅢ
					クラスⅣ

図1.3.6　厚生労働省の医療機器に係わるカテゴリ

関与したJIS規格を、**図1.3.7**に示す。当JIS規格は、安全に関する規格であり、機器の効用や効果に関するものではない。また、JIS T 0601-2-208の電位治療器に関しては、規格化にあたり3年遅れた。JIS規格審議の方針としては、以下の7つを考慮した。①国際規格がある場合は、それとの整合性をとり、②国際規格が無い場合は、世界にも通用する規格とする。③業務用と家庭用ＪＩＳで、矛盾・重複がないように考慮する。④本ＪＩＳ規格のみで内容理解ができるように、わかりやすくする。⑤技術的内容を主に審議する。⑥原案作成委員会の委員構成における下準備を完璧にしておく。⑦経済産業省との綿密な事前・事後調整を行う。

また、JIS審議の運営においては、以下の4つを考慮した。①審議方針の共通事項化を行う。②ＪＩＳ審議期間予定し、期間内の終了を目指す。③理解を早めるため、「まず、○○○治療器とは何か一言で説明して下さい。」というように治療器の概要から理解することとする。④内容を理解できるように、解説を先に審議することとする。

以上のJIS審議を踏まえてJIS化を行った。

JIS T 0601 -2-

3:2005	超短波療法機器	IEC60601-2-3翻訳規格
5:2005	超音波物理療法機器	IEC60601-2-5翻訳規格
35:2005	医療用ブランケット、パッド、及びマットレス加湿装置	国内独自規格
201:2005	水治療法用圧注装置及び温浴療法装置	国内独自規格
202:2005	紫外線治療器	国内独自規格
203:2005	赤外線治療器	国内独自規格
204:2005	空気圧式マッサージ器	国内独自規格
205:2005	医療用マッサージ器	国内独自規格
206:2005	乾式ポットパック装置	国内独自規格
207:2005	キセノン光線治療器	国内独自規格
208:2008	電位治療器	国内独自規格

図1.3.7　関与したJIS規格

医療機器の第三者認証制度（**図1.3.8**）が2005年4月から開始された。以前の医療機器は、厚生労働大臣の承認が必要であった。そこで、低リスク医療機器のうち、厚生労働大臣が基準を定めた品目について、厚生労働大臣の承認を不要とし、第三者認証機関が基準への適合性を認証する制度を導入するものである。第三者認証制度とは、基準認証等の制度において、自己確認を基本としつつ、ある程度の危害発生の蓋然性が認められるものについて、補完的に第三者の確認を義務付ける仕組みである。したがって、クラスⅡの指定管理医療機器等については、民間の第三者認証機関で認証審査業務が行えるようになった。

・テュフズードジャパン
・（財）日本品質保証機構
・（財）医療機器センター　等

平成21年2月25日時点で１２の第三者認証機関が存在している。

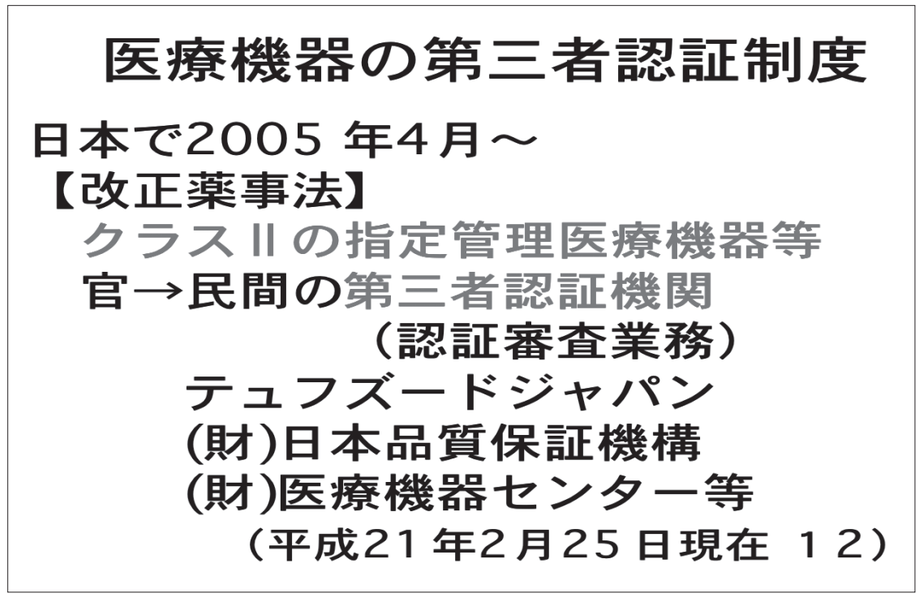


図1.3.8　医療機器の第三者認証制度

国際的な試験所認定規格「ISO/IEC 17025（JIS Q 17025)」に基づき、(財）日本適合性認定協会(JAB)、(独法）製品評価技術基盤機構(NITE)、(独法）認証センター(JNLA)に認定された試験所は公的試験所と同等の試験所とみなされる。「ISO/IEC 17025」は、電気、機械・物理、化学など技術分野毎に認定基準を定め、審査に適合した場合に認定する規格で、試験所は、この中の試験所及び校正機関の能力に関する一般要求事項に基づき認定されることになる。試験所として認定されると、第三者認証機関の認証は不要となる。JABより試験所認定を受けているのは、オリンパス㈱、フクダ電子㈱等、JNLAより試験所認定を受けているのは、(財）自動車産業振興協会技術研究所等が挙げられる。

また、例えばオリンパス㈱品質保証部試験評価センターは、国際MRA対応事業者（**図1.3.9**）となっている。国際MRA（Mutual Recognition Arrangement）とは多国間の相互承認のことである。国際相互承認は、参加している認定機関の間で相互評価（ピアレビュー）を行い、認定機関の運営が国際的な基準であるISO/IEC 17011に基づき行われており、ISO/IEC 17025を認定基準として使用していることが評価される。JCSSは平成11年にILAC/APLACの相互承認に署名をしており、国際的な基準に適合した認定機関の運営が評価されている。

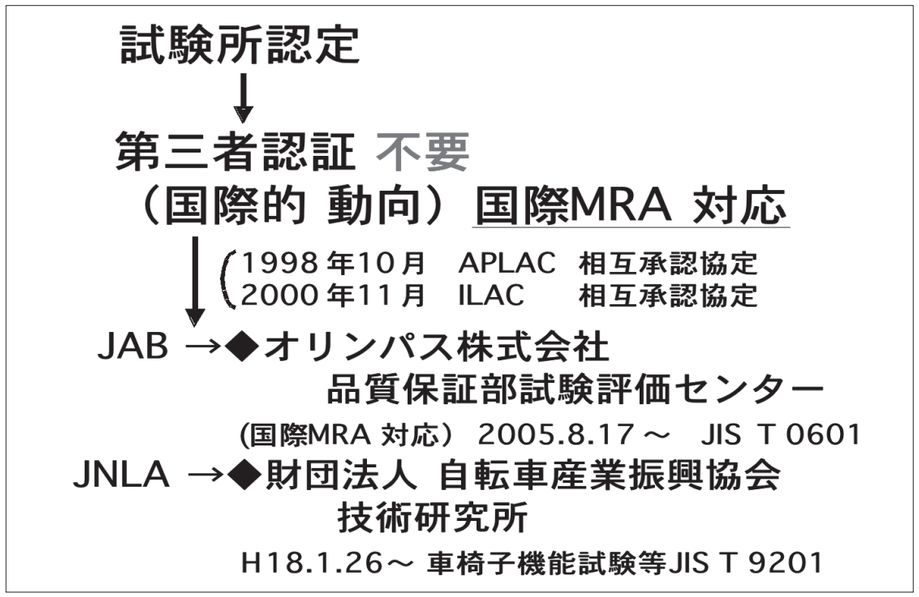


図1.3.9　国際MRA対応事業者

以上をまとめると、生産者、使用者、中立者のご支援により無事にＪＩＳ化を完成できた。これらに基づいて理学療法機器が実用化されることで社会貢献につなげていきたい。また、今後も問題点や改善事項が生じた時は、速やかに見直しを行い、真に役立つＪＩＳ規格としていきたいと考えている。

1.4　安全への取り組みと日本への導入事例紹介（シーメンス社）

本節は、シーメンス株式会社産業オートメーション ＆ ドライブテクノロジー事業部オートメーションシステム部雨宮祐介氏のご協力を得て、レポートをまとめたものである。

連絡先 ： シーメンス株式会社
産業オートメーション ＆ ドライブテクノロジー事業部オートメーションシステム部
〒141-8641 東京都品川区東五反田3-20-14高輪パークタワー17F
E-mail: yusuke.amemiya@siemens.com
URL: http://www.siemens.co.jp/ad/
Tel ： 03-5423-8673　Fax ： 03-5423-8734

1.4.1　シーメンス社と機能安全の係わり

1880年代からシーメンス社は、自動制御の安全を確実にすることは人間の義務であり経済的にも意味があると提唱してきた。近年では以下に示すように国際安全規格の策定に積極的に関与している。

1) IEC TC65 ： Industrial Process Measurement and Control（工業プロセス計測制御）
Roland Heidel氏がチェアマンとして参加
そのほか下記の通りメンバーとして参加
SC 65A - System aspects ：（システム側面）
WG14,MT 61508-1/2 & 3
関連規格 ： IEC 61508, IEC 61511
SC 65B - Measurement and control devices
WG 7 - Programmable control systems（計測制御機器）
関連規格 ： IEC 61131(プログラマブルコントローラ)シリーズ
例、IEC 61131-3 PLCプログラミング5言語
SC 65C - Industrial networks
WG 12 - Functional Safety for Fieldbus（デジタル通信）
関連規格 ： IEC 61784-3-3 工業用ネットワークのファンクショナルセーフティ通信のプロファイル

2) IEC TC44: Safety of Machinery - Electrotechnical aspect（機械類の安全性－電気的側面）
Friedrich Harless氏がチェアマンとして参加
そのほか下記の通りメンバーとして参加

WG 7 Safe control systems for machinery
関連規格 ： IEC 62061（機械類の安全性－安全関連の電気 ・ 電子 ・ プログラマブル電子制御システムの機能安全）
WG 11 Requirements for semiconductor manufacturing equipment
関連規格 ： IEC 60204-33（機械類の安全性－機械の電気装置－第33部 ： 半導体製造装置に対する要求事項）
MT60204-1 Safety of machinery- Electrical equipment of machines-Part 1: General requirements
関連規格 ： IEC 60204-1（機械類の安全性－機械の電気装置－第11部 ： 交流1000V又は直流1500Vを超え36kV以下の高電圧装置に対する要求事項）

3) シーメンスドイツの活動/ IEC TC44
ISO/TC199/WG 6 Safe control systems
関連規格 ： ISO 13849-1 and -2:
ISO/TC 199/WG 5 Risk assessment
関連規格 ： ISO 14121
リエゾングループ（Liaison Group）ISO 13849-1/IEC 62061
その他、関連するDINやEN会議にも参加。

1.4.2　安全設計の概要

欧州機械指令：
機械やプラントのメーカーは設計時、リスク評価、分析を行わなくてはいけない。安全規格に準拠し、安全設計された機械だけがマーケットに出すことが許される。(CEマーキング)
安全設計のプロセスは規格によって定められている。原則的に以下のプロセスをたどって行われる。

1. リスク評価/分析
リスク評価/分析とは設備の危険源を洗い出し、それぞれの危険源に対して損害の大きさ、危険源にさらされる時間、頻度、回避の可能性を評価、分析し危険源から要求される安全レベルを決定することである。(ISO 12100、14121参照)

2. リスク軽減
ここでは、リスク分析された危険源に対し、3つの手法で安全対策を行う。①本質安全設計、②安全防護及び付加保護、そして③使用上の情報である。

3. リスクの容認

リスクの軽減はその時の一般社会の価値観などを考慮して、容認できる小さなリスクまで危険度を小さくする必要がある。また、文書とテストによってそれを証明しなければならない。

安全設計プロセスにおいて、実行の為の厳密な指示は国及び地域の規格によって若干規格が異なっている。機械及びプラントが運用される国及び地域のガイドラインと規格を参照することが重要である。

1.4.3　関連国際規格と規格の発展

過去異なった国で生まれた規格は調和され、そしていくつかのヨーロッパの規格へと移行しその後国際規格へと移行した。日本国内でも代表的な機械安全規格であるヨーロッパ規格EN954-1の有効期間は、2011年12月31日までであり、2012年からはISO 13849-1に移行する。

現在国際規格として代表的な関連規格は以下の通りである。

1）代表的な国際規格とその内容

IEC 61508（JIS C 0508 ）■ 機能安全の基本規格

IEC 61511(JIS C 0511) ■ プロセスエンジニアリングのアプリケーション規格

IEC 62061(JIS B 9961) ■ 機械エンジニアリング及び安全関連の電気・電子・プログラマブル電子制御システムの機能安全のアプリケーション規格

ISO 13849-1(JIS B 9705-1) ■ 機械エンジニアリングと電気 ・ 電子と他の技術(e.g. 空圧、水圧)のアプリケーション規格（EN 954-1から移行.）

IEC 61800-5-2(JIS化予定) ■ 安全機能が統合されたドライブの製品に特化した規格

IEC 62061 とISO 13849-1は機械のリスクアセスメントに使われる。

IEC 61508 とIEC 61800-5-2は安全ドライブのリスクアセスメントに使用される。

2）規格の発展

例 ISO 13849-1 : 2006

EN954-1 (ISO13849-1 : 1999)はセンサー、アクチュエータの2重化などハードウェアの構成のガイドラインとなっていたが、今回の改訂でIEC 61508のように機能安全の概念を取り込み、機器の故障確率や危険側に故障する平均時間など時間的な部分も考慮されるようになった。

1.4.4　規格の階層構造

基本安全規格（A規格)、グループ安全規格（B規格)、個別機器の安全規格（C規格）の3層構造をなしている。

A規格（ISO 12100）

根本的な要求と全ての機械の定義が書かれており、“機械の安全、根本的な要求、一般的な基本設計原則”がふくまれている。

B規格

代表的な規格としては IEC 62061、IEC 61508、IEC 61811などがあり、さらに特定の安全性側面に関するB1安全グループ規格と、B2安全関連装置に関する規格の二つに大別される。B規格はC規格を則る上で第1の目標となり、具体的なC規格がない場合、メーカーの機械の設計の助けとなる。

C規格

特定の機械類に対する詳細な安全要件を規定する規格であり個別機械特有の規格。例えば木工機械、エレベータ、工作機械など。

1.4.5　安全コンセプトの開発

以下規格に定められた安全コンセンプトの開発について順を追って説明する。

(1) マシン設計

制限を決め、機械を使用するための文書化を行う。初期のスタート手順、安全要求事項、プロダクトの文書化、利用者マニュアルなど。

(2) リスク分析/リスクアセスメント

危険のタイプ、場所、起こりえる結果を文章化しリスクの結果、リスクの大きさ、そしてリスク軽減の可能性によってリスクアセスメントを実施する。

リスクアセスメントのチャートはリスクアセスメントフローチャートと呼ばれる。リスクの軽減は既述の通り以下の順番で行う。即ち①本質安全設計、②安全防護及び付加保護、③使用上の情報（３ステップメソッドとも呼ばれる）である。

(3) 要求される安全レベルの決定

要求される安全レベルの決定は、概略次の3つの規格それぞれにリスクグラフがあり、そのグラフから決められる。

1. EN954-1によるCategoryの決定
2. ISO 13849によるPerformance Level (PL) レベルの決定
3. IEC 62061によるSafety Integrity Level (SIL)の決定

参考　リスクの大きさは次の結果により決定される。

・怪我の度合（重傷 軽傷）

・危険にさらされる時間、頻度（頻繁もしくはまれ長時間もしくは短時間）
・危険回避の可能性（困難もしくは可能）

本件については後述するが正確な計算は規格によって異なるので注意が必要である。

（4）必要な安全機器構成の決定

上記の開発ステップを経過し、それぞれの危険源から要求される安全レベルに対して必要な安全機器構成の決定をすることになる。

1. ISO 13849-1

機械類の安全制御システムに要求される原則や性能を規定した規格。

ここでは安全レベルをPL（Performance level a--e）とし、各レベルの要求事項や対策安全関連の数値の計算方法などが記載されている。

2. IEC 62061

機械類の安全性－安全関連の電気・電子・プログラマブル電子制御システムの機能安全。ここでは、安全レベルをSIL（Safety Integrated level）1--3で規定する。

危険側故障確率（PFHd）とは、装置に発生する故障のうち安全側に倒れる故障ではなく、かつ診断手法により検出できない故障確率であるが、この計算は安全機器の決定の大きな要素である。

安全コンセンプトの開発のプロセスの概要は以上であるが、特に重要な点に関連する規格には以下のものがあげられる。

（1） SIL ： IEC 62061

（2） PL ： ISO 13849-1

ここでは安全関連パフォーマンスレベルの評価は、Ｓ、Ｆ、Ｐの３つの要素で決定される。すなわち ：

Ｓ　：損傷レベル
Ｓ１：軽度（通常修復可能な）損傷
Ｓ２：重度（通常修復不可能）損傷
Ｆ　：危険にさらされる頻度及び／または時間
Ｆ１：まれに～比較的高頻度及び／または短時間
Ｆ２：高頻度～継続的及び／または長時間
Ｐ　：危険を回避できる可能性
Ｐ１：特定条件により可能
Ｐ２：ほとんど不可能

（3）危険側故障確率の計算：ISO 13849-1及びIEC 62061では安全機器の危険側故障確率を計算し、規格に規定されているそれぞれの安全レベルで要求される確率を満足す必要がある。

1.4.6　シーメンス社のセーフティーサポート

“新しい”機能安全要求を実行することはお客様にとって“チャレンジ”であるとともに機能安全要求を実行する効率の良いソリューションを探しているとの考えのもと、以下のようなセーフティーサポートサービスを提供している。

1)サポートツールの提供

セーフティエバリュエーションツール、機能安全自動計算ツール

安全機能を検証するためのインターネットベースの無料ツールはISO 13849-1のPL、IEC 62061のSIL 両規格に対応しており、その特徴は ：

シーメンス製品の最新情報を提供、両規格ともに変わらない操作、結果をレポートとして文書化ということにあり、その詳細は以下のURLを参考にされたい。

www.siemens.com/safety-evaluation-tool

2)セーフティサポートサービスの提供

ファクトリーオートメーションとプロセスオートメーションで異なる規格と法規を扱う二つのサービスパッケージを提供している。

1. SIL、PLの検証（危険側失敗確率（PFH、PFD）の計算を含む）
   ガスコンプレッサステーションにおける過圧保護、温度保護、防火の安全関連機能を対象にしたSILの検証が、プロジェクト実施の際のSILの検証の一例である。
2. 安全プラン、ドキュメント、検証、バリデーションなどからなる安全ライフサイクルマネージメント。
3. 機能安全を要求されるIEC 62061 及びISO 13849-1規格を伴ったサポート。
4. システムインテグレータ向けトレーニングコンセプトの開発。
5. 顧客のアプリに特化したトレーニングと安全用ファンクションブロックの開発

例としては、安全PLCシステムを利用した発電用安全ファンクションブロックの開発があげられる。

1.4.7　シーメンス社の安全製品

基盤製品としては安全リレー、ASIsafe、モジュラーセーフティーシステム（ MSS)、安全PLCなどがあげられる。シーメンスは30年以上前からをマーケットにこれらの安全製品を提供し続けている。 以下がその主なラインアップとその年度である。

1980　SIMATIC S5-110F
1988　SIMATIC S5-115F
1994　SIMATIC S5-95F
1999　PROFIsafe for PROFIBUS, SIMATIC S7-400FH
2005　PROFIsafe for PROFIBUS & PROFINET

安全PLCはプログラミングによる高い柔軟性を実現するとともに二重化診断処理という最新テクノロジーによってより安全性を向上させている。また、CPUについて言えば、以前はプログラムの二重処理を行うためには２台のCPUが必要であったが、SIMATIC S7-300Fでは１台のCPU（1つのプロセッサ）で２重処理を行える。ソフトウェアのコンパイラはユーザープログラムから逆の論理に変化し、またWORDロジックに変換し診断用のプログラムを生成し、このことによってDiversity（多様性）を満たしている。

安全関連の通信は、2つのPROFIBUSとPROFINETバスシステム上で、標準の通信と同じように行われる。IEC 61508を満たした安全通信プロトコルであるPROFIsafeプロファイルを使うことで、これらの通信がフェールセーフ通信用に拡張される。しかも安全関連の通信と標準の通信は、同じケーブル上で行える。

PROFIsafeプロファイルは以下の機能によりアドレス異常、通信速度の低下、データ誤送などを検出する。すなわち、パケットへのシリアル番号割付、通信の時間監視機能、ノード毎のユニークなアドレス設定によるステータス監視、CRCチェックである。

これらを使用した安全制御の例としては、備え付けられたカメラによる映像を利用したクレーンアプリケーションでの実施例を**図1.4.1**で示す。

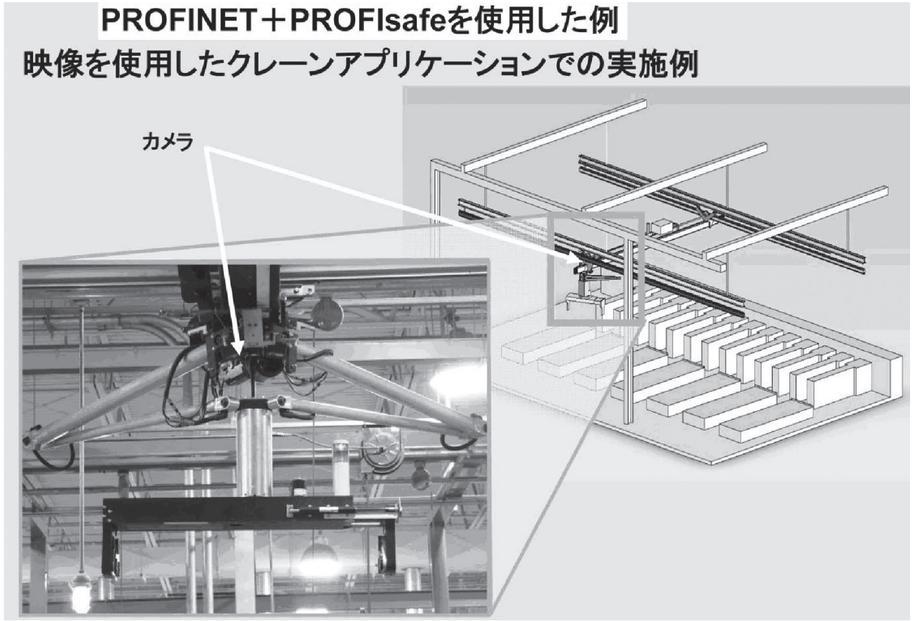


図1.4.1　クレーンアプリケーションでの実施例

1.4.8　日本への導入事例

工業炉（連続熱処理炉）

工業炉の安全はJIS B 8415工業用燃焼炉の安全通則によって規定されている。そのポイントはリスクアセスメントの実施と火炎監視装置にはプログラマブルコントローラ（PLC）を用いてはならない、インターロック回路には従来使用していたPLCは使用不可で、公的に認められた安全PLCのみ使用可能ということになる。

本PLCは完全ブラックボックスでユーザーによるプログラム変更が出来ず、当然ながらプログラマブル機能を有していない。

「安全プログラマブルコントローラ」を使用しない場合、ソフトウェアだけによる燃焼安全のインターロックを構成してはならないとされている。ここで、安全プログラマブルコントローラとは、JIS C 0508-1のSIL2又は、SIL3の安全機能をもつ公的に確証されたプログラマブルコントローラをいう。シーメンス燃焼安全コントローラはこれに対応している。

当システムにおける主要な使用ソフトは下記の通りである。

STEP7 V5.4 日本語Ver. PLCエンジニアリングツール

Distributed safety V5.4 安全PLCエンジニアリング用Add-onソフトウェア

バーナーパッケージフェールセーフバーナーファンクションブロックパッケージ

S7-PLCSIM V5.4 PLC用オフラインシミュレータ

1.5　セーフウェア/安全 ・ 安心なシステムとソフトウェアを目指して

本節は、株式会社日本機能安全　吉岡律夫氏のご協力を得て、2010年8月23日に行われた講演に関するレポートをまとめたものである。

連絡先 ：
株式会社日本システム安全研究所
代表取締役　社長
〒234-0053　横浜市港南区日野中央3-17-24
TEL:045-832-5103
FAX:045-832-9277
E-mail:ritsuo.yoshioka@nifty.ne.jp

1.5.1　セーフウェアとは何か

実証された技術やノーハウを導入しても、「そのノーハウやマニュアルがなぜできたか？」という背景を学ばなければ、本当には役に立たない。安全の分野においても、過去の広い産業システムにおける失敗や事故を学び、これらを防ぐ仕組みがなぜできたかを納得する必要がある。

この講演で紹介する「セーフウェア」という本は、米国MITのレブソン教授によって書かれ、コンピュータを活用する各種のシステムにおいて、「失敗や事故はなぜ起きる？これらを防ぐ仕組みは何か？」を教える教科書である。

著者のナンシー ・ レブソン教授は、MITの航空宇宙工学部門に所属し、「ソフトウェア安全」という新分野を創設し、現在も世界の第一人者である。

「セーフウェア」はレブソン教授の造語であり、原因が複雑化、コンピュータ化、組織化したシステム事故を防ぐためのものである。システムとは、ハードウェアやソフトウェアという技術的要素と、人的要因や組織管理 ・ 安全文化という非技術的要素から成り、システム事故を防ぐには、これらのすべての要素に対する安全、つまり「システム安全」を実現しなければならない。

1.5.2　事故はなぜ起きる？

交通分野や化学プラント事故の70から80%は、現場員のミスに起因するとされている。しかし、ヒューマンエラーは事故の原因ではない。不適切な設計、組織、教育などの結果である。

信頼性と安全性は同義ではない。たとえば、自動車のエアバッグを例に取ると、正面衝突ではエアバッグが作動して無事であるが、側面衝突ではエアバッグは作動するが、運転手は死亡するという事故が起きる。後者では信頼性は十分だが、安全設計が不適切だった。

リスクとは、部品やシステムが持つ潜在的な危険性であり、事故の大きさと事故の頻度の組合わせとして認識される。近年は、この概念が浸透し、リスクを低減しても、許容できるリスクのレベルがさらに下がってきている。

事故の発生は、**図1.5.1**に示す三層モデルで説明できる。ベースに根幹原因があり、環境 ・ 条件が重なり、直接の原因が起きると事故になる。

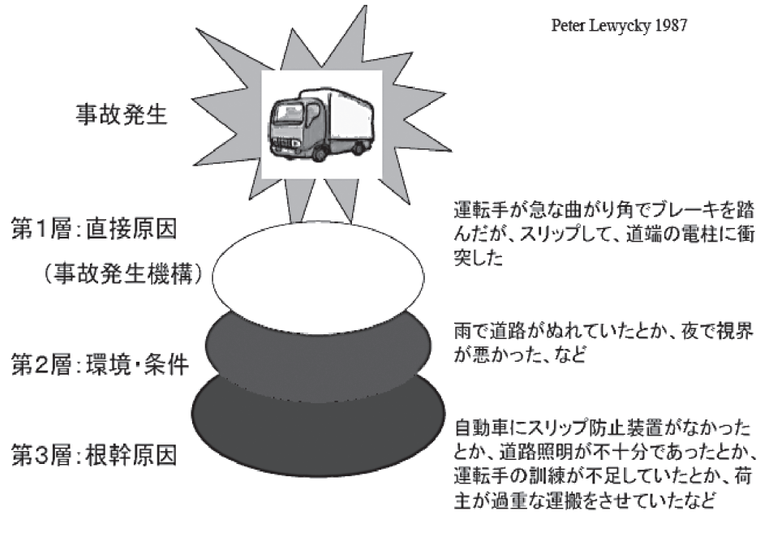


図1.5.1　事故の三層モデル　　出典：講演資料

1.5.3　事故の根幹原因

事故の根幹原因(Root Cause)は次の3カテゴリーに分けられる：

- 安全文化の欠陥
- 組織構造の欠陥
- 技術活動の欠陥

この中で、安全文化の欠陥は、さらに次のように分けられ、この講演ではこれらによる影響を述べる：

1. 自信過剰と自己満足
   (1) リスクの過小評価
   (2) 冗長性に頼りすぎること
   (3) 非現実的なリスク評価
   (4) 低確率で過酷な事象の無視

(5) リスクの経年減少を仮定
(6) ソフトウェア関連リスクの過小評価
(7) 早期の警報や兆候の無視
2. 安全に低い優先順位を割当てること
3. 経済性目標との間違った解決

(1) リスクの過小評価（独立事象仮定の誤り）

自信過剰と自己満足は、現代の主要な事故で共通の要素である。実際、スリーマイル島事故では、「技術が安全であると繰返し保証された結果、装置が故障しないことについて固定観念を持っていた」と証言されている。スペースシャトル・チャレンジャー号事故では、「安全性に対する要求が、通常のシャトル運用では少なかったという自己満足と信念が、事故の関連原因である」と指摘されている。

自己満足の一つの面は、リスクを過小評価するという基本的な人間の傾向である。リスクを予測しようとするとき、明示的にあるいは暗黙の内に、各事象に独立性を仮定してかけ算をし、極端に低い確率値を得ようとする。しかし、実際には事象の独立性がないことが多い。

タイタニック号の事故がこの例である。過去の実績では16防水区画のうち、4区画以上が破損したことはないので、本船は絶対に沈没しないと信じられたが、実際、氷山に横向けに衝突して、5区画以上が破損し、沈没した。

(2) 冗長性に頼りすぎること（共通原因故障の問題）

冗長性と多様性が、失敗を避けようとして、また信頼性を増やそうとして、しばしば使われる。しかし、停電や火災のような一つの要因が、すべての機器を同時に故障させるかもしれない。多くの事故が、冗長あるいは多様なシステムにおいて、共通原因故障により起きている。

1985年の御巣鷹山の事故では、事故機には4系統の油圧操縦系があったが、同じ場所を通っていたために、すべて破壊されて操縦不能に陥った。

(3) 非現実的なリスク評価（確率論の限界）

確率論的リスク評価は、特定の設計が妥当かどうかについて決定する場合のみ、有用である。設計変更がリスクを減らすために必要かを示す目的で使うことができる。しかしながら、間違って用いられ、得られた低い確率値のせいで、自信過剰をもたらす。数値解析では、数値化できるものだけを使用するので、設計エラーや管理エラーのような数値化できない因子は無視されがちである。

テラック25放射線照射装置の過剰照射事故において、確率論的リスク評価では事故はあり得ないとされたが、ソフトウェアエラーが除外されていた。

(4) 低確率で過酷な事象の無視

最もありそうな潜在危険は対応が取られるが、潜在危険が重大であっても、その確率が低いと仮定されると、検討する値打ちはないとして無視される。しかし、事故が起きてみると、事象の独立性が間違っていた、あるいは確率論的評価が非現実的であったことに初めて気づく。

(5) リスクの経年減少を仮定

結局は自己満足に過ぎない信念とは、「何年もの間、事故無しで運転しているから、そのシステムが安全であるに違いない」という思い込みである。重大な事故がなければ、リスクが減少しているように見えてしまう。

1967年のアポロ1号事故の対策を講じて、事故を避けることに成功したと自負してしまい、安全より任務遂行に重点を置くようになった。その結果が、1986年のチャレンジャー号事故になった。

(6) ソフトウェア関連リスクの過小評価

ハードウェアの安全装置は、多くのシステムでソフトウェアによって置き換えられつつある。しかし、多くの機械的安全装置は、十分に試験され、信頼性が高く、そしてフェールセーフで、物理学の単純な原則に基づいている。これらをソフトウェアで置き換えることは間違っている。ソフトウェアが機械的インターロックの良い特性をほとんど持っておらず、複雑さと相互干渉を増やす傾向があるからである。

(7) 早期の警報や兆候の無視

自己満足の最後の問題は、事故の前兆や警告を真剣に受取らないことである。実際、事故が起きる前に、公衆からの警告や一連の小さい事象がよくある。たいていのシステムは、単一故障や単一エラーを処理するように設計されており、潜在危険に至る前に修正されてしまう。これらの早期警報や兆候の無視が、事故に繋がる。

(8) 安全に低い優先順位を割当てること

(9) 経済性目標との間違った解決

担当者に自信過剰と自己満足がなくても、経営者が安全に十分な予算と人員を当てなければ、重大な事故が起きる。利益、生産性、スケジュール等の経済性とのトレードオフを考慮して、最初から設計しておかないと、えてして経済性が優先され、事故に繋がる。経済性と安全性は車の両輪であり、バランスが狂うと事故を誘発する。

総じて、「安全文化」とは、「用心深さ」の文化と言える。

1.5.4　ヒューマンエラー

事故後の調査で「事故原因はヒューマンエラー」とされることがほとんどであるが、事故防止のために、背景の技術的要因、組織的要因を解明する必要がある。ヒューマンエラーは事故の原因ではない。

ヒューマンエラーを防止するために自動化が行われるが、安易に容易なことだけを自動化すると、人の能力が低下してしまい、緊急時に対応できなくなってしまう。機械の故障と、ヒューマンエラーを相互に助け合うシステムを設計すべきである。

1.5.5　システム安全

システム安全の基本概念は、**表1.5.1**のとおりである。

この表の第2項に関連するが、安全装置をつけると、「もう事故は起きない」という過信が生まれる。ある日、この安全装置が故障して、さらにひどい事故が起きたり、想定外の事故が起きる。設計者は、安全装置をつければ安全と考えてはならない。

表1.5.1　システム安全の基本概念　　出典：講演資料

1	システム安全は、予見できる事故を防止し、予測できない事故の影響を最小限にするために、システム工学手法を用いる。
2	システム安全は、完成した設計に安全を加えるのではなく、**設計に安全を組み込む。（・・とは言っても⇒次頁）**
3	システム安全は、機械・人間・環境（管理者・設計者なども含め）など全体としてのシステムを扱う。
4	システム安全は、**ハザード（潜在危険）**を単なる機械の故障以外にも想定する。**（ハザードとは何か⇒後述）**
5	システム安全は、過去の経験や規格よりも、**起こるかも知れない事故に対する分析**を重視する。
6	システム安全で重視されるのは、定量的手法よりも**定性的手法**である。
7	システム安全は、安全性と、効率・性能・使いやすさ・費用などの他の目標との**トレードオフ**を重視する。

システム安全設計の進め方を**表1.5.2**に示す。この表に関連して、ハザードとは何かを説明すると、次のように説明できる：

- ●従業員、住民、乗客などの健康や生命に物理的被害を与える潜在的な危険源。潜在危険とも呼ぶ。
- ●爆発、火災などの事象をいい、未だ発生していない状態であり、実際に発生すると事故となる。

表1.5.2　システム安全設計の進め方　　出典：講演資料

1	システム安全管理を確立すること（前頁）
2	ハザード分析の実施（システムにおける危険は何か？）（13章～15章）
3	ハザードを除去すること（本質安全設計）
4	ハザードを低減し、制御する設計の採用（16章）
5	ヒューマンエラーを考慮したインターフェース設計（17章）

ソフトウェアに関しては、**表1.5.3**に掲げるような神話があるが、いずれも誤りである。ソフトウェアには次の2種類のエラーがある：

- ●ソフトウェアに対する要求事項が間違っていた
- ●ソフトウェアが要求仕様通りに作成されていなかった

コンピュータが関わる安全問題は、ほとんど前者である。しかし、既存のソフトウェア工学は、ほとんど後者のみを扱っている。ソフトウェアエラーに対する対策は次の通りであり、セーフウェアの本の中で解説している：

- ●ソフトウェアを修正して、完璧なものにする
- ●ソフトウェアにエラーがあっても、耐えられるようにする
- ●システムのリスク分析など、システム安全工学に基づく標準的手法（セーフウェア手法）を採用する

表1.5.3　ソフトウェアの7つの神話　　出典：講演資料

1	コンピュータのコストは、アナログ機器や電気機械装置より安い。
2	ソフトウェアは「簡単に」変更できる。
3	コンピュータは置き換えた電気機械装置よりも高い信頼性を提供してくれる。
4	ソフトウェアの信頼性が高まれば、安全性も高まる。
5	ソフトウェアを試験すること、または（形式的手法を用いて）ソフトウェアが正しいものであると証明することで、全てのエラーが除去できる。
6	ソフトウェアを再利用すれば安全性が高まる。
7	コンピュータは機械的システムよりリスクが少ない。

1.5.6　結論

まとめとして、システム安全のための11箇条を**表1.5.4**に示す。

表1.5.4　システム安全のための11箇条　　出典：講演資料

1	安全をより確かなものにする最も効果的な方法は、単純であることと、知的に処理できるシステムを構築することである。
2	安全性と信頼性は別のものであって、混同してはならない。
3	確率論的リスク評価に依存し過ぎるのは賢明でない。管理や組織問題など、数値で表せないものがある。
4	システムに安全を最初から組み込むことは、完成後に防護装置を加えるよりも、はるかに良い結果が得られる。
5	事故の根幹原因に対処しなければ、事故の再発は殆ど防げない。技術的問題に加えて、管理上や組織上の欠陥問題も考慮しなければならない。
6	単に人間をコンピュータに置き換えても安全問題は解決しない。 人間のエラーは人間の創造性・柔軟性と不可避に結び付いているので、コンピュータを用いて人間の能力を増強すべきである。
7	安全はシステムの問題であるので、異なる分野の専門家が協同することが必須である。特にソフトウェア(SW) 技術者は、システム安全の概念と技法を理解し、一方、システム安全担当者は、SW 開発に係わる必要がある。
8	SW の安全性は、その SW が動作するシステムの中でのみ、評価することができる。SW 単独で見てはいけない。
9	自己満足は最も重要なリスク要因であり、それを最小にする安全文化が確立されなければならない。
10	ハザードを分析し、除去し、経済性等の他要因とのトレードオフを考慮してリスクを低減すること。あるいはその情報を示すこと。
11	われわれは同じ過ちを繰り返さないよう、過去から学ばなければならない。

■参考文献

1）「セーフウェア　安全・安心なシステムとソフトウェアを目指して」原著：Nancy G. Leveson、監訳：松原友夫、翻訳：片平真史・吉岡律夫・西　康晴・青木美津江、2009年

2）「リスクにあなたは騙される」、Dan Gardner、2009年

3）「だから失敗は起こる」畑村洋太郎、2007年

4）英国健康安全庁、「COST of ACCIDENT」

5）J. リーズン「保守事故」、2005年

6）D.T. McRuer、「The Human Operator as a Servo System Element」、1959年

1.6　安全に寄与するための分析、設計、検証手法の展開

本節は名古屋市工業研究所 小川清氏のご講演を元に、まとめたものである。

1.6.1　概要

＜背景＞

愛知県は交通事故死日本一を継続中である。そこで、安全なシステム構築というものが必要であろうと考えた。具体的には、次のような関係組織から、指導を受けたり、協働することとした。

JAXA、日本機能安全、産業総合研究所から指導を受け、地元企業と協働を行ってきた。

交通事故原因については、原因別交通死亡事故［**図1.6.1**］。

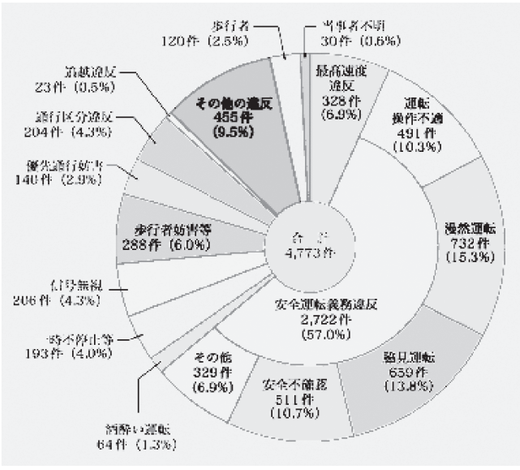


図1.6.1　原因別交通死亡事故

特にソフトウェア関連事業について考えた場合、課題として、

- 分析をしたことがない人が多い
- 設計指針が明確でない
- 責任感の欠如
- 技術者の基本的技術スキルの低さ

ということが挙げられる。

設計指針が明確でないことは、ツール等の現状から分析することもできる。例えば、

- MISRA-Cはあるが、それは主に可搬性のためのものである
- PolySpace Verifierはあるが、手が届かない
- MatLabはOS, ネットワークとの連携が不十分である。したがって、現場で、設計指

針を明確に持つということは難しい。

また、責任感の欠如、次のように現れている

・試験設計を設計者が実施しない
・国際規格を貿易障壁であると誤解している
・国際規格は認証をとるだけのものだと誤解している
・手を動かさない管理者が威張っている

これらは、責任感の欠如であり、技術者は規格の意味などは正しく理解し、また、試験について考えることもなども設計者の責任範囲であることを認識すべきである。

今日の技術者は、技術のための基本的な技法が身についていない。例えば、

・コンピュータ(状態機械)を対象とした仕事をしているのに、状態遷移図(state chart)を描いたことがない
・通信系、関数呼び出しのプログラムを書いているのに、時系列図(sequencediagram)を書いていない
・離散(デジタル)システムを設計しているのに、刻時図(timing chart)を描いたことがない
・ソフトウェア、システム設計をしているのに分析、設計審査(review)を体系的にしたことがない

など、今日のソフトウェア開発現場は、危ない状況である。

これではいけない。日本の強みを伸ばすべく努力しよう。

1.6.2　設計と分析

設計と分析を行うが、そこには設計指針が必要である。

設計指針が無いままに分析を行った場合、設計と分析が行ったり来たりを繰り返し、設計がいつまでも定まらない。

HAZOPとUMLは分析と設計との道具である。

設計は図、言語で記述する。

分析は量、質、時間、順序などについて行う。

検証は事前条件、事後条件を比較する。検証はエンドレスに行え、それを自動化するようになっている。

(1)視点の違いによる誤解

各人の立つ位置と、視点によってものごとは異なった見え方をする。そして誤解が生まれる。

互いの視点の違いを認識しないと、議論が互いにかみ合わず、堂々巡りになってしまいがちである。

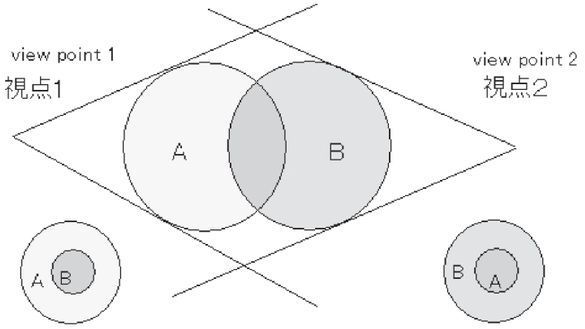


図1.6.2　視点による認識の違い

誤解を減らすためには、用語について考えなければならない。一つの言葉を2つ以上の意味で使っていないだろうか? 例えば、「b」という単語を、blueやbitの意味で使用したら、人間は文脈からその単語が何であるか理解する。しかし、各人の立ち位置によって、文脈は異なることがあり、誤解を招く原因となる。

用語を階層構造で定義することができる。集合関係を用いて、文の意味をより厳密に表現することが可能である。

例えば、オブジェクト指向パラダイムの「継承」は、単に継承というだけでは、is-a関係なのか、has-a関係なのかわからないという曖昧性が指摘された。よって、現在では、集合関係を用いて、「継承」を、厳密にはis-a関係かhas-a関係かでいうべきである。

このように、集合関係を用いれば、用語を厳密に定義することが可能になることがある。

is-a関係

A is a B. (AはBである)

これは、AがBに包含される包含関係を表す。

has-a関係

B has a A.

AはBのメンバ・フィールド中にある。

Aであるオブジェクトの振る舞いは、その所有者の規則によって決まる。

has-a関係とは、あるオブジェクトにおいて「メンバ・フィールド」と呼ばれるオブジェクトと、それを含むオブジェクトとの関係である。

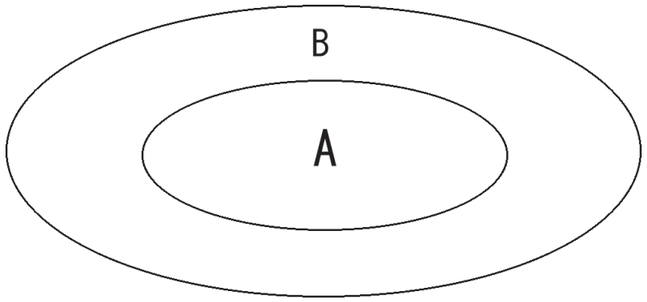


図1.6.3　is-a関係。A is-a B

（2）ソフトウェアの品質特性

ソフトウェアの品質特性を分類したISO/IEC 25000シリーズがある。品質というものを定義し、改善についても定量化を行っている。

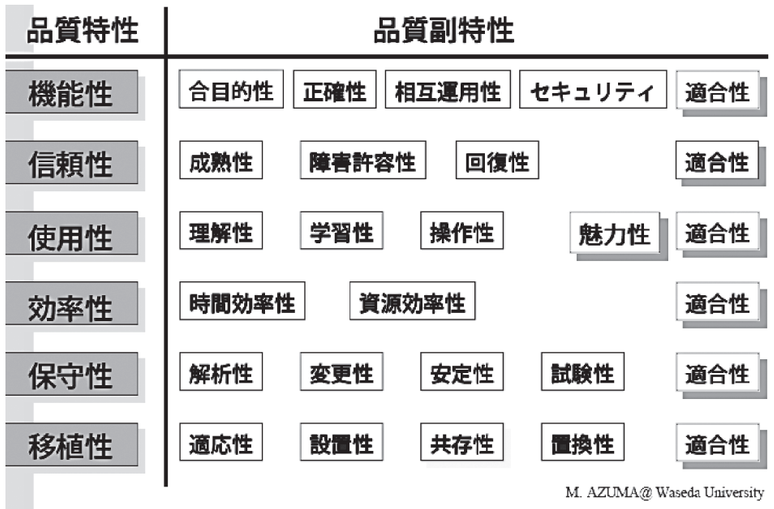


図1.6.4　ISO/IEC 25000シリーズ（早稲田大学 M.Azuma氏による）

利用時の品質（quality in use）には、「利用時の要求（requirements）」と「意図した利用（intended use）」がある。

利用時の要求（requirements）の場合、それを満たすかは「検証（Verification）」を行う。意図した利用（intended use）の場合、それを満たすかを調べるのは、「妥当性確認（Validation）」である。

利用時の要求は最低限、必ず満たされるべきものである。意図した利用は、より広い。最近は、意図が重視される。

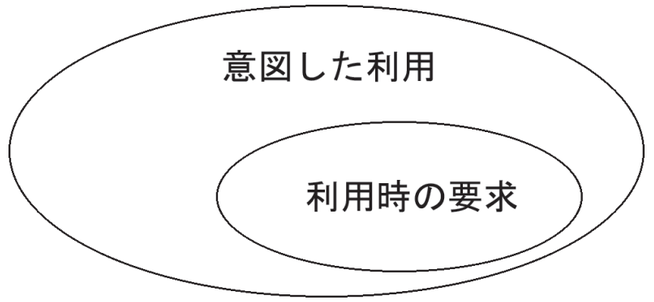


図1.6.5　利用時の品質

改善を定量化することは、ISO/IEC 15504 part2 で行われている。

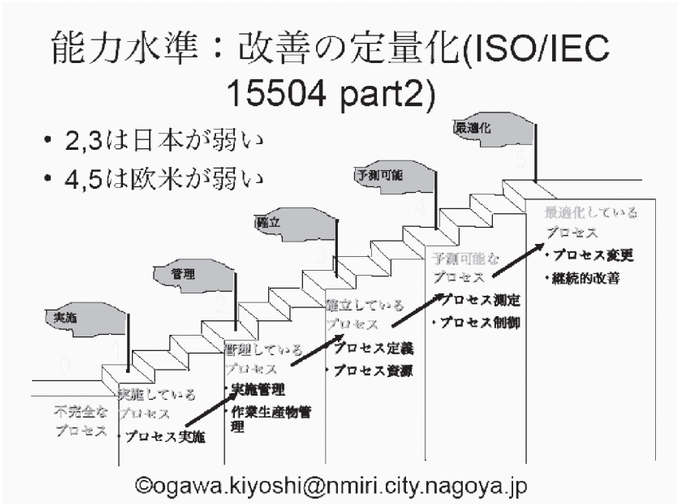


図1.6.6　能力水準

ISO、IEOなどの品質関連規格の関係は次の図のとおりである。

	ISO9000対応ガイド	ISO/IEC 15504に基づく診断モデル
ISO/IEC 15288システムプロセス	ISO/IEC TR 90005	ISO/IEC TR15504-6
ISO/IEC 20000運用プロセス	審議開始	ISO/IEC TR 15504-8 CD審議中
ISO/IEC 12207 ソフトプロセス	ISO/IEC90003	ISO/IEC 15504-5
自動車分野	ISO TS16949	Automotive SPICE(?)

図1.6.7　品質関連規格の関係

（3）標準化

国際標準は実効的に意味があるにも関わらず、それに関わる全員が正しく意義を理解していないと、標準にまつわる弊害が出る。それを第三者認証制度にまつわる「負のスパイラル」として、表現したのが下図である。

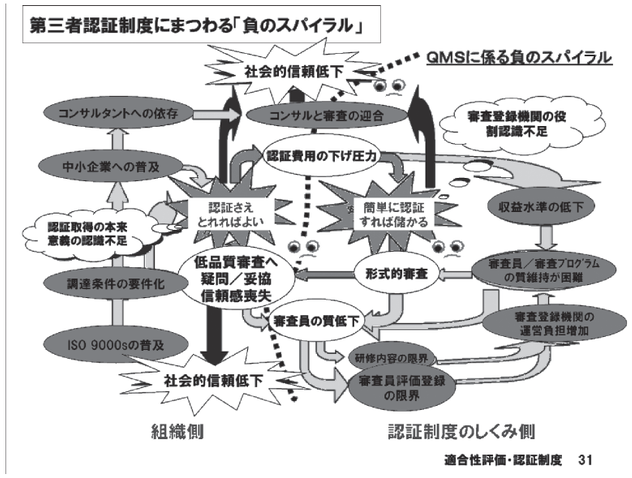


図1.6.8　第三者認証制度にまつわる「負のスパイラル」 ©日本規格協会 ： 国際標準研修

JAXAでは、HAZOPを分析/設計よりも後で使用している。名古屋市工業研究所ではあらゆる段階でHAZOPを使用している。

（4）設計指針

下記のような国際規格を道具としてとらえる

- IEC HAZOP(hazard analysis and Operability Study)
- ISO DIS 26262 Road vehicle - Function Safety
- ISO/IEC 17050-1,2 この規格適合は自己宣言で

設計指針の検討するときに、標準規格に沿って運用し、規則を定めることにする。

例えば、設計指針として「かたちの規則」が必要で、それは例えば、ユニバーサルデザインがある、そこには、「JIS 高齢者 ・ 障碍者配慮設計指針」という規格があるので、それを参照して規則を決める。これが、標準規格を道具として使うということである。

かたちの規則に、ソフトウェアに当てはめると次のようになる。

- 統一と変化(unify)：変更想定

- 単純(simple)：関数、単体試験
- 均衡(balance) ： データ量と計算量
- 比率(proportion) ： 計算時間
- 調子 (rhythm) ： 制御構造
- 強調(accent) ： 検証上重要な事項
- 調和 (harmony) ： 複雑さの分布
- 対称(symmetry) ： 記述言語、製品の対称性

ユニバーサルデザインとは、下記を満たすような設計である。

- 誰にでも公平に使用できること
- 使う上での自由度が高いこと
- 簡単で直感的にわかる使用方法となっていること
- 必要な情報がすぐに理解できること
- うっかりエラーや危険につながらないこと
- 無理な姿勢や強い力なしで楽に使用できること
- 接近して使える寸法、空間となっていること

（5）HAZOPとUML

以下では、HAZOP(Hazard analysis and operability study)とUML(Unified Modeling Language)について述べる。

HAZOPは、危険 ・ 運用分析である。処理変数(process parameter)と誘導語(guide word)で分析を行う。分析は経験に基づく。網羅的な事象の列記が可能で知識の体系化が可能になっている。

処理変数とは、

速度、方向、重量、温度、振動、電磁ノイズ、湿度、重量分布、風速

などである。

誘導語は、

無、過大、過小、部分、尚早、遅刻、事前、事後

であり、程度の評価を表す。

誘導語は、ある対称軸について、その軸上での正と負で、対称性が求められる。代表的な対称軸について対象な誘導語の例を示す。

表 1.6.1　誘導語の対称性

正	反	対称軸(axis)
-	無(no)	存在 (existence)
-	逆(reverse)	方向(direction)
大(more)	小 (less)	量(quantity)
類(As well as)	部(Part of)	質 (quality)
前(before)	後 (after)	時間(time)
早(early)	遅(late)	順序(order)

赤信号停止システムを例にとって、HAZOPを適用してみる。赤信号停止システムは、図1.6.9のように、無指向性無線と指向性無線の2つを使用するシステムである。

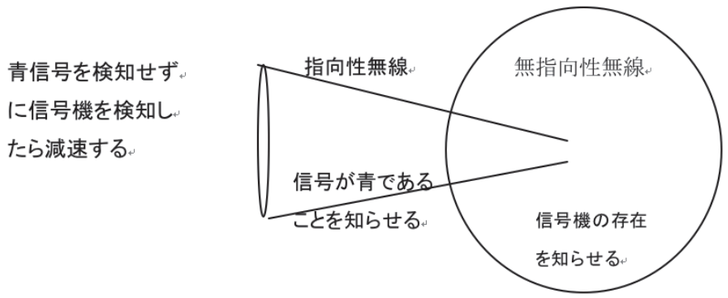


図1.6.9　赤信号停止システム

		無	過大	過小	部分	尚早	遅刻	事前	事後
パラメータ	速度	○	○	○		○	○	○	○
	方向	○				○	○	○	○
	重量	○	○	○				○	○
	温度	○	○	○		○	○	○	○
	振動	○	○	○		○	○	○	○
	電磁ノイズ	○	○	○	○	○	○	○	○
	湿度	○	○	○		○	○	○	○
	重量分布	○			○	○	○	○	○
	風速	○	○	○		○	○	○	○

図1.6.10　時系列図の例

識別	事項	現象	差 (ずれの内容)	ずれの原因	システムへの影響	安全対策
1	電磁ノイズ	過大	信号が受信できない	他無線機によるノイズ	信号の見落とし	無線の二重化
1	風速	過大	信号機が発信しない	信号機の電源供給停止	信号機の機能停止	目視運転
21	振動	過大	指向性無線が発信しない	断線	信号機の一部機能停止。青信号を検知せずに信号機を検知する。すべての車が減速し、渋滞を引き起こす	目視運転

図1.6.11　分析例

図1.6.10、**図1.6.11**のように、分析ができる。分析によって、気がつかず、見落としそうな危険を発見できる。そして、その危険について対策を行う。

危険を洗い出す時には、通常ありえないようなことも考えて、チームの全員でどんどんと案を出す。その後、常識的な範囲で発生しそうな危険について、分析を行う。発生の確率の低いものは、分析が簡単であることが多いので、実際に分析を行うときは、発生確率の低いものから手をつけると、気が楽になれる。

分析時は、発言は必ずすべて記録し、抹消しない。それが検討済みで対策不要と結論付けたというエビデンスとなるからである。同じような案件を何年も分析していると、同じようなことを言う人が必ず出現する。そういう人の発言も、ちゃんと記録することが大事である。

UML図の効能

UML図表として、状態遷移図(state chart)、時系列図(sequence diagram)、刻時図(timing diagram)、有方向グラフなどが描ける。下に、UML図表と誘導語の対応を示す。UMLには、矢印を書く。その向きについて逆の分析ができる。どんなUML図の線も矢印として向きを入れる。

表1.6.2　UMLと誘導語

UML 図表	対応誘導語	備考
ユースケース図(ユーザを含めて書く)		
時系列図 (sequence diagram)	順序、時間	
状態遷移図 (state chart)	順序	
刻時図(timing di agram)	時間	エレベータのタイミングなどもこの図で
有方向グラフ	逆	矢印が大事

一人HAZOPのすすめ

通常は、チームで行うHAZOPを一人で行う。一人HAZOPは低コストで実施できる。以下に、ある事例で、2回繰り返しでHAZOP作業を行ったときのコスト、3回繰り返しでHAZOP作業を行ったときのコストを掲げる。

表1.6.3　一人HAZOPの活用例(1)2回繰り返しでHAZOP作業

	記録	座長	利用	保守	安全	合計
準備の一人 HAZOP	6					6
Reviewの二人HAZOP	3	3				6
班構成の HAZOP	3	3	3	3	3	15
一人 HAZOP	18		18			36
統合の二人 HAZOP	3		3			6
班構成の HAZOP	3	3	3	3	3	15
合計時間	36	9	27	6	6	84
単価	1.2	1.5	0.8	1	2	
費用	43.2	13.5	21.6	6	12	96.3

表1.6.4　一人HAZOP適用例(2)3回繰り返しでHAZOP作業

	記録	座長	利用	保守	安全	合計
準備の一人 HAZOP	4					4
Reviewの二人HAZOP	2	2				4
班構成の HAZOP	2	2	2	2	2	10
一人 HAZOP	12		12			24
統合の二人 HAZOP	2		2			4
班構成の HAZOP	2	2	2	2	2	10
一人 HAZOP	18		18			36
統合の二人 HAZOP	3		3			6
班構成の HAZOP	3	3	3	3	3	15
合計時間	48	9	42	7	7	113
単価	1.2	1.5	0.8	1	2	
費用	57.6	13.5	33.6	7	14	125.7

このように、一人HAZOPで整理をして意識を高めておけば、チームで総合的にHAZOPを行うコストが非常に小さくなる。

一人HAZOPを行うときには、色々な立場で考えることが大事である。自分の立場だけで考えると、自分の考えをうまく説明できない人が多いが、一人HAZOPで色々な立場に立って考えておけば、説明がうまくなる。

そのために**図1.6.12**のような「HAZOPさいころ」を考案した。これを眺めながら、立場を変えながら、HAZOPを行う。

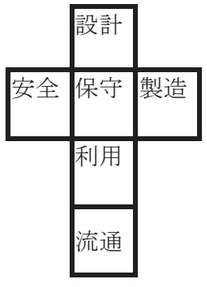


図1.6.12　HAZOPさいころ

（6）まとめ

HAZOPを実施することによってFTA,FMEAでは発見できなかった事項がみつかることがわかった。また、誘導語に対称性があることに着目してHAZOPを利用すると、整理の作業がはかどることがわかった。UMLにもとづいて図を作ることによって作業に無駄がなくなる。

また、一人HAZOPを実施することにより、全体での作業が効率的になることがわかった。

HAZOPの誘導語の課題として、

・「As well as」,「質の増大」とはソフトウェアの場合、何が該当するのか

・「Other than」は「reverse」と対応づけした方がよいのか

がある。

1.6.3　検証

検証をどうして使用するか。その要因は主に下記である。

・ 人手だと限りがない分析

・ 状態遷移だけでも検証したい

・ 形式的に記述すれば検証できることも多い

（1）名古屋市で取り組んできた形式手法

・ SPIN(simple promela(protocol/process meta language) interpreter)

・ Z(ISO/IEC 13568:2002 Information technology -
Z formal specification notation - Syntax, type system and semantics)

・ VDM(ISO/IEC 13817-1:1996
Information technology - Programming languages, their environments and system software interfaces - Vienna Development Method Specification Language - Part 1: Base language)

・ Event-B(B method)

・ UPPAAL

・ Alloy

（2）UPPAAL

UPPAALでできることは、次のようである。状態遷移図を描き、その状態遷移をシミュレーションして、時系列図の例を描く。状態遷移で到達しないところがあるかを確かめる。時間を記述して時間関係における矛盾がないことを確かめる。

（3）SPIN

SPINで実施されていることは、次のようなことがらである。状態遷移からpromeraの自動生成（富士ゼロックスでの実例）。これは主にassertの生成に注目している。SPINは、状態遷移表からpromelaの自動生成する。

（4）Alloy

Alloyセミナ実施（実績）

株式会社豆蔵 小林健一氏に、

1. Alloyの特徴（Alloyの位置づけと理論背景）

2. 文法速習（最低限の文法解説＆例題実施）

3. 実例紹介（図＆モデルによる解説）を講演を実施し、演習を名古屋市工業研究所にて行った。

1.6.4 まとめ

実際の世界では、設計、分析、検証、試験は同時進行で起こっている。つまり、V字モデルに基づくことは、ナンセンスである。故障分析 ・ 安全分析で、状態遷移図、時系列図、刻時図を使うと有効であることがわかった。安全分析結果から検証、試験事例を作成するのがよい。

■参考文献

- 5ゲン主義入門，古畑友三，日科技連出版社，1996
- なぜなぜ分析徹底活用術，小倉仁志，JIPMソリューション，1997
- 4M5E, http://http://www.n-iinet.ne.jp/4m5e.htm
- FMEA、FTA実施法、鈴木順二郎、日科技連，1982
- 名古屋市工業研究所研修テキスト，2008
- μITRON4.0仕様書、TRONプロジェクト
- MISRA-C - C解説書、日本規格協会、2004年 ・ 2006年

1.7 宇宙分野のソフトウェアの安全確保の取り組み

本節は、独立行政法人宇宙航空研究開発機構（JAXA）情報 ・ 計算工学センター安全 ・ 信頼性推進部に所属されている片平真史ソフトウェアエンジニアリングチームリーダのご協力を得て、レポートをまとめたものである。

連絡先 ：

独立行政法人宇宙航空研究開発機構（JAXA）

情報 ・ 計算工学センター　安全 ・ 信頼性推進部

〒305-8505　茨城県つくば市千現2-1-1

TEL:050-3362-3791

FAX:029-868-2987

URL:http://www.jaxa.jp

1.7.1 宇宙分野のソフトウェアの概要と特徴

宇宙分野のソフトウェアは、人工衛星、宇宙ステーション、ロケット、地上設備など多岐にわたる。ロケットは、打ち上げ時に万が一軌道からずれるようなことがあればすぐさま破壊しなければいけないし、人工衛星の場合には、運用時に放射線によるデータ化けが発生する可能性も考慮する必要がある。また、宇宙ステーションのシステムには、人が介在するため、ロケットや人工衛星よりもさらに複雑なシステムとなる。

例えば、ロケットのシステムでは常に多数決をしながら飛んでいる。HTVは結果的にうまくいったが、運用中にいくつか問題も発生した。しかし、問題が発生した場合の対処を検討していたためにうまくいったと考える。なぜならば、事前にソフトウェアのライフサイクル全般についての標準であるISO 12207に従って意識合わせを行っていたからである。

1.7.2 ソフトウェア信頼性向上に向けた活動全般

ソフトウェア独立検証及び有効性確認IV&V(Independent Verification & Validation)やモデルベース開発も研究している。一般にシステムを冗長化すれば安全になると言われるが、かえって安全ではなくなる。というのも以前、多くの機能を追加したことにより、組み合わせが増え複雑になったからである。そして、結局、検証することが出来なかった。使用頻度の増加に比例して新たなハザードも増加するが、航空機事故の例のように必ずしも自動化は必ずしもよくないことがわかる。

1.7.3 ソフトウェア神話について

ソフトウェアの７つの神話のなかでも特に以下の４つの神話を信じてはいけない。

●神話２ ： ソフトウェアは簡単に変更できる。

●神話４ ： ソフトウェアの信頼性が高まれば、安全性も高まる。
●神話５ ： ソフトウェア試験、または形式的手法により正しいものと証明することですべてのエラーが除去できる。
●神話６ ： ソフトウェアを再利用すれば安全性が高まる。

神話２については、ソフトウェアは簡単に変更できるものではない。なぜならば、変更を実施すると、それまでに行ったプロセスをもう一度行わなければいけないからである。これには莫大なコストがかかる。

神話４については、ソフトウェアエラーの除去だけでは安全性は高まらない。たとえ100%の信頼性でも事故が起きることがあるからである。よって、テストがすべてではない。なぜならば、要求されているものが間違っている場合を考慮するとテスト自体が意味のないものになってしまうからである。

神話５については、形式的言語で記述する時点で間違ってしまう場合を考慮すると自明である。

神話６については、ソフトウェアは特定の環境を前提として開発されているので、条件が異なるとそのままでは再利用できないからである。

1.7.4　安全文化の欠陥

安全を意識した文化を構築することが重要である。1960年代から、宇宙分野ではいろいろな事故が発生している。

例えば、チャレンジャー事故では責任と権限が隠れた要因である。コロンビア事故もタイルが剥がれていることがわかっていたのにも関わらず、大気圏に再突入させたことが原因である。

1996年6月4日に発生したアリアン501の事故では、発射から37秒までは正常に飛行したが高度3700m付近で突然、予定していた飛行経路を大きく逸脱し爆発した。複雑な要因が重なったことにより、再利用したソフトウェアの使っていない部分が動作したために異常な値を出力してしまったのが原因である。

1999年9月23日の NASA マーズサーベイヤ98計画では、メートル法とヤードポンド法を間違えて使用してしまった。これは、宇宙分野ではよくある間違いであり、実はJAXAでもあった。

1999年12月3日の NASA マーズサーベイヤ98計画では、センサーの振る舞いなど、ソフトウェア要求仕様に欠陥があった。これは、ソフトウェア設計者の理解不足が原因であったが、果たしてソフトウェア設計者に理解させることが妥当かは疑問である。

1999年4月30日の 米Titan IV B-32では、設計を変更しないために不要なソフトウェアを使用していたうえに、情報伝達のミスが発生した。ある値がおかしいことに技術者が気づき、上司の留守電にメッセージを残したが、上司が聞いたのは爆発後であった。

1.7.5　事故の分析

国家運輸安全委員会（NTSB）モデルでは、事故の原因として組織的因子、寄与因子、直接因子がある。JAXAでは、事故モデル分析を用いた不具合分析を行っており、システム因子（Systemic Factor)、寄与因子（Contributing Factor)、直接因子（Direct Causal Event）に分けて、数百件、数千件の改善箇所の優先順位をつけて対策を行っている。

人間の重要な役割について、特にヒューマンエラーを考慮する必要がある。例えば、スリーマイル島原子力発電所事故では警告が100個以上鳴ったことにより、最初は何が起きたのかわからなかった。よって、自動化システムにおける人間の役割についてメンタルモデルを十分に考慮しなければいけない。つまり、オペレータが訓練できるような分野では良いが、回転ドアなどの不特定多数が使用するシステムの場合、事前に使い方を考慮する必要がある。

1.7.6　定義

事故、インシデント、ハザードという用語について以下のように定義する。

●事故 ： ある特定のレベルの損失を引き起こす、望ましくない、そして計画外の事象（かならずしも不測の事態ではない）
●インシデント ： 損失は伴わない（あるいは軽微な損失のみを伴う）が、異なる状況下では損失の可能性がある事象
●ハザード ： システムの環境における他の条件をもたらし得るシステムのある状態、または一部の条件

つまり、人間の怪我や死亡のみが事故ではなく、ハザードはシステムまたはコンポーネントの環境に対して定義される。

1.7.7　国際宇宙ステーション計画における安全要求

安全（評価）プロセス要求と安全技術要求の両方が必要である。

安全（評価）プロセス要求では、

①安全確保の体制
②安全解析手法
③安全審査プロセス

等を定め、組織的且つ系統的なアプローチによる「安全確保の進め方」を規定している。

一方、安全技術要求では、

①共通の要求（基本的な考え方や共通事項など）
②個々のシステムに特有の要求

等が全体システムの仕様の一部として要求される。

そして、安全技術要求が満たされているかを評価するプロセスにおいて安全を確立する。

1.7.8　宇宙ステーションにおけるハザードのカテゴリと要求される故障許容数

事象発生時の影響の大きさは、下表のようにカタストロフィック（致命的)、クリティカル（重大)、マージナル（軽微）の3つのカテゴリに分けられる。

事象発生時の影響の大きさ(カテゴリ)	ハザードの被害の度合い	故障許容設計適用時の故障許容数
カタストロフィック（致命的)	能力の喪失に至る人間の傷害、致命的な人間の傷害。またはスペースシャトル、宇宙ステーション、あるいは主要な地上設備の喪失の原因となりうる状態。	2 故障許容
クリティカル（重大)	重度な人間の傷害、もしくは重度の職業上の疾病をもたらす状態。宇宙ステーションエレメント、軌道上の生命維持機能、あるいは緊急システムの喪失の原因となりうる状態。	1 故障許容
マージナル（軽微)	安全監視機能、緊急制御機能、または緊急システムの重大な損傷。応急手当を要する人間の軽度の障害。打ち上げまたはサービスビークル、主要な宇宙ステーションエレメント、軌道上の生命維持機能、地上設備、あるいは全てのクリティカルな地上支援装置の軽度の損傷を伴う状態。	故障許容は要求されない

発生頻度が低いものは、NASAの安全審査では考慮されない。カタストロフィックとクリティカルの問題についてのみ議論される。

1.7.9　宇宙分野のハザード分析と安全審査

開発プロセス毎に安全審査プロセスを規定しており、概念設計はフェーズ0、基本設計はフェーズ1、詳細設計はフェーズ2、試験後はフェーズ3となる。

システムレベルでは、フェーズ0でトップ事象（ハザード）の識別（システムFTAによる分析)、フェーズ1でシステムFTAなどによる原因と制御方法の識別、フェーズ2で制御方法の詳細/検証方法の検討、フェーズ3では設計結果の反映/検証結果が行われる。

ソフトウエアレベルでは、フェーズ0で関連するソフトウェアの識別、フェーズ1でソフトウェアFTAによる関連（原因、制御方法）個所の識別、フェーズ2で該当箇所に対するソフトウェア安全要求の適用、フェーズ3で設計結果の反映/検証結果が行われる。

しかし、ソフトウェアは故障しないのでFTAを行っても意味がない。よって、動作すべきものが動作し、動作しないものが動作しないことを確認している。

1.7.10　安全評価プロセス

以下のように安全（評価）プロセスを規定している。

1．　STEP1 ハザードの識別
2．　STEP2 ハザードの原因の識別
3．　STEP3 ハザードの除去/制御
4．　STEP4 ハザード制御の検証

STEP1（ハザードの識別）およびSTEP2（ハザードの原因の識別）では、予測可能なすべてのハザードを「事象発生時の影響の大きさ（Severity)」と「事象の発生頻度」とともに網羅的に抽出する。次に抽出されたハザードの原因を識別する。この解析作業は、対象となるハードウェア、ソフトウェア、運用、誤操作等のヒューマンエラー、インターフェース、環境条件等を考慮し、

●一般的に考えられるハザードリスト(JSC26943、NSTS/ISS 13830)
●ハザード識別表
●フォールトツリー解析（FTA)
●故障モードと影響評価解析（FMEA)
●フォールト伝搬解析（ソフトウェアのみ)

を活用して実施する。

一般的ハザードリスト
汚染（CONTAMINATION ）
腐食（CORRO SION ）
電気ショック（ELECTR ICALS HOCK ）
火災（FIRE ）
爆発（EXPLOSION ）
衝突（COLL ISION ）
傷害・病気（INJ URY AND ILLN ESS）
放射線（RAD IATION ）
温度異常（TENPE RATURE EXTREM ES）
オービタ突入能力の喪失（LO SS OF OR BITER EN TRY CAPAB IL ITY）
出典：JSC26943 、NSTS/ISS 13830

JEM（Japanese Experiment Module : 日本実験棟）におけるFTAの例として、酸素圧、物体の衝突による破損、ロボットアームの暴走等があげられる。

ソフトウェアがハザードに関連するケース（宇宙ステーション）を2つあげる。ケース１は動かないことが原因で危険な状態になるケースである。これは、口の周りの二酸化炭素を吸うと数秒で死に至る空調システムや消火システム等があげられる。ケース２はソフトウェアが原因でシステムが異常動作するケースである。これは、ロボットアームの暴走等があげられる。自動車のエアバッグは両方のケースに分類されるだろう。

STEP3（ハザードの除去/制御）では、ハザードの除去 ・ 分離、ハザードの制御を行う。

ハザードの除去 ・ 分離では、識別されたハザード（たとえば、シャープエッジなど）を除去 ・ 分離する設計を行う。現実的にはハザード除去が出来ない場合に、以下の優先順位でハザード制御を行う。

①ハザードを最小にする設計
　１．故障許容設計 ： ハザードカテゴリに対応した故障許容設計（2又は1故障許容）
　２．リスク最小化設計 ： 適切な部品 ・ 材料の選定および適切なマージンの確保により、発生しうるハザードが最小になるようにする。
　NASAでは、ハザードを最小にする設計のみが認められる。
②安全装置 ： 異常が発生したときでも被害を最小にするように安全装置を付加する。
③警報 ・ 非常装置 ： 異常時に乗員が速やかに対応できるような非常設備および防護具を備える。
④運用手順 ： ハザードが最小になるような運用手順を整備する。
⑤保全 ： 適切な予防保全により以上の発生頻度を小さくする。

　STEP4（ハザード制御の検証）では、STEP3の「ハザードの制御」が「意図したとおりに働く（機能する)」ことを、試験、解析、検査、デモンストレーションの何れか或いはその組み合わせによって確認する。

1.7.11　安全性構築技術と事例紹介

　耐故障性を考慮し、部品レベル、装置レベル、ボードレベル、サブシステム ・ システムレベル、統合システムレベルというように各レベルでの対応が必要である。

部品レベル	放射線対策 EDAC　（回路レベルとともに）
装置レベル、ボードレベル	部品・回路レベルの冗長化 装置自己故障診断及び回復 ソフトウェア故障診断及び回復 ソフトウェア耐性設計（信号の冗長化、有効性チェック、ベストエフォートなど）
サブシステム・システムレベル	装置・系（計算機、センサー）レベルの冗長化 多数決システム 故障診断及び回復 安全モード自動移行 自動化、自律化
統合システムレベル	宇宙機システムの詳細診断 地上などからの処理支援（自動、人間） 人間の介入

1.7.12　コンピュータシステム安全技術要求(SSP50038)の事例

　たとえば、コマンドを2回入力すること等が要求される。また、不意に動いてはいけないような場合では、OS以外はモジュールを分けるなどの要求がある。
また、設計検証においては、計算結果が正しいかを検証するなどの対応が求められる。

1.7.13　独立検証及び有効性確認（Independent Verification and Validation: IV&V）

　IV&Vとは、製品の正しさ及び品質をライフサイクルを通して評価するためのシステムエンジニアリングプロセスである。
　検証(Verification)では、各段階の開発中間成果物が、前の工程からの入力情報に照らし、正しく作られていることを確認する。
　妥当性確認(Validation)では、各段階の開発中間成果物が、JAXAが期待する通り（システム要求や安全要求を満たしているか）に作られていることを確認する。
　戦略的開発 ・ 検証計画において、インプロセスによる検証では開発中に検証する。また、V&Vによる検証では、完成後にチーム内で検証する。しかし、IV&Vによる検証では、異なる会社の人達が異なる方法論で検証する。
　検証技術としては、チェックリスト、モデル検査、独立試験等で評価を行う。ロールやピッチなどの入力で極性の誤りがよく発生することがあるので、考えられる原因に特化するようなチェックリストを作成している。
　IV&Vでは、技術的な独立性が求められる。そして、なるべくフロントローディングを行い、早い段階でバグを潰すことが重要である。さらに、製品が要求通り作られているかよりも、エラーが発生しないように作られているかの方が重要である。

1.7.14　選択的ソフトウェアIV&V手法

　IV&Vでは莫大な作業時間になるが、工夫すると短縮することができる。それが、選択的ソフトウェアIV&V手法である。例えば、完全性 ・ 一貫性を検証するためには、通常はチェックリストを使用するが場合によっては、モデル化/モデル検査を行うことでシミュレーションまでは不要になることもある。整合性、正当性の検証では意図的に故障を入力して検査を行ったり、内製ツールを活用している。
　また、開発プロセスとSpecTRMによる安全評価の研究も行っており、SpecTRMを用いた一貫性 ・ 完全性評価の事例では、バルブ異常の時に緊急停止出来ない事象を発見したり、バルブ異常の時に緊急停止コマンドが出力されても緊急停止しないことが判明した。
　モデル検査においてモデル化段階では人が不具合を発見できるが、一貫性解析や完全性解析では人が見つけられない不具合を検出することができる。つまり、システムエラーを見つけることができる。抽象度を抑えたモデル化が重要であるが、決してモデル検査だけに頼ってはいけない。人がレビューすることと組み合わせることが何よりも重要である。

一度モデルを作成しておくと役に立つ。システムの複雑さ、環境の変化に伴う問題を考慮すると、今後は、新たなハザード解析方法が必要となるだろう。

1.7.15　米マサチューセッツ工科大学における最新研究

米マサチューセッツ工科大学（MIT）のNancy Leveson教授の最新研究では、これまでのハザード解析技術（FTA等）では抽出しにくかった事象を抽出し、システムの複雑さに起因するシステムエラーを見つけることができる。それが、STAMPとSTPAである。

●STAMP（Systems-Theoretic Accident Model and Processes：安全解析のためのモデル）

●STPA（STAMP-Based Hazard Analysis：安全解析手法）

HAZOPが物理的構造中心に対して、これらは制御（機能的）構造であるのが特徴である。

1.7.16　まとめ

以上、宇宙分野のソフトウェア安全の取組を紹介したが、重要なことは、安全プロセスに従うだけではなく、設計・解析手法を適用することだけではなく、ソフトウェアシステムがどのようにハザードに関わるのか、そして、それを顕在化させない方法を考える（真の安全確保）ことである。

1.8　機械安全設計手順と安全コンポーネント

本節はオムロン株式会社オートメーションシステム統轄事業部セーフティ事業部に所属されている河野秀明主事の御協力を得て、セーフティ・リレーの設計における「機械安全設計手順と安全コンポーネント」に関するレポートをまとめたものである。

1.8.1　オムロン株式会社の活動概要

創業以来70年近く制御機器の開発と製造を中心としたグローバル企業で、世界で「安全と安心」で信頼のブランドとして高い評価を受けている。

機能安全の面では、「センシング＆コントロール」と「安心をカタチに」をビジョンに技術開発を行い、安全に関する取組みから信頼性の高い製品も高評価を得ている。

同社の事業は次の5種類が有り、どの事業も「機能安全」とは深い関わりを持つものばかりである。

①制御機器・FAシステム事業

FA(ファクトリーオートメーション）のパイオニア

②電子部品事業

高精度・高機能な電子部品や電子デバイスの開発

③車載電装部品事業

カーエレクトロニクス技術

④社会システム事業

便利で安心・安全な、公共、交通、セキュリティ分野のソリューションとサービス

⑤健康医療機器・サービス事業

ホームメディカルケア機器やサービス

連絡先：

本社　京都市下京区塩小路通堀川東入
オムロン京都センタービル
TEL 075-344-7000

大崎事業所　〒141-0032　東京都品川区大崎1-11-1
ゲートシティ大崎ウエストタワー14F
TEL 03-5435-2000

URL：http://www.omron.co.jp/

1.8.2　労働災害防止の考え方

労働環境は、他人種の外国人労働者、事業所の海外展開などにより変化するし、その変化に合わせた労働災害の防止策が必要となる。

（1）労働災害防止の基本

労働災害防止のためには、技術変化による機械の変化および、設備環境の変化を含めた安全策を講じる必要があり、災害が発生した時の社会的影響および、社会的責任も十分に考慮しなければならない。

人間の作業空間と機械の作業空間とが重なる危険領域があり、基本的な災害防止のためには空間、時間、あるいは両方を分離することが重要である。（**図1.8.1**）

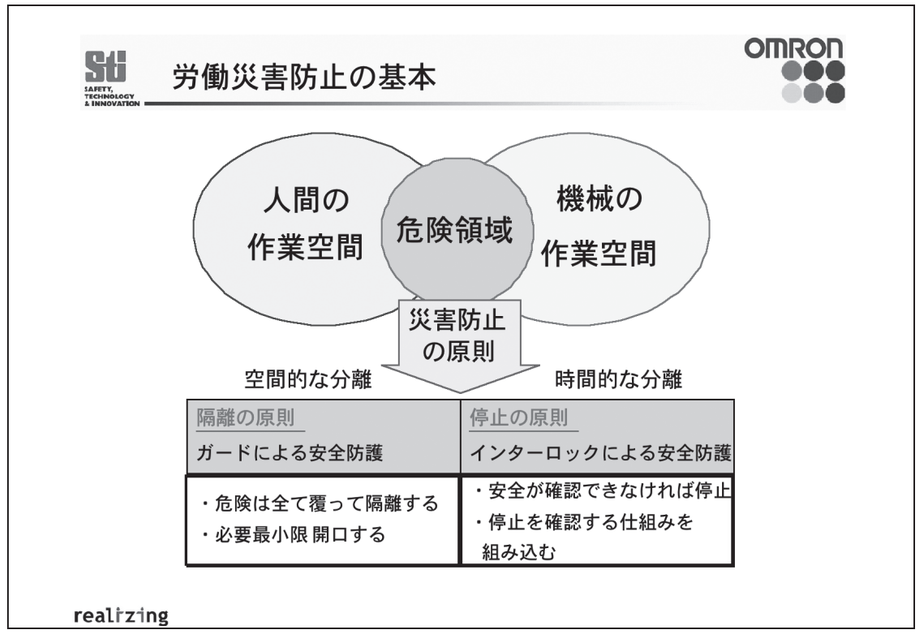


図1.8.1　労働災害防止の基本（出典 ： オムロン社資料）

（2）安全構築の考え方

労働災害防止のための安全構築の考え方として、「災害ゼロ対策」に加えて「危険ゼロ予防」の考え方が必要となる。

1) 災害ゼロ ： 起こった事への対策としては以下のものがある。

①教育訓練

②指示徹底

③作業者責任

2) 危険ゼロ ： 起こりえる事への予防策としては以下のものがある。

①本質安全設計

②安全な機械の導入

③企業責任

（3）安全方策の考え方

災害防止の安全方策を考えには次の項目を前提に考える必要がある。

①人は間違える　 ： 作業経験にかかわらず安全を確保する。

②機械は故障する ： 現場調整／保守時も安全を確保する。

1.8.3　機械安全に関する国際規格と日本の状況

機械安全に関する国際規格は、ISO/IECにて多くの規格があり、その解説は他の章に譲り、ここでは「規格の活用」と「厚生労働省の指針」について解説する。

（1）国際規格の活用について

装置の使用者及び装置メーカーは、国際規格を共有ガイドとしてコミュニケーションをとることが重要である。（**図1.8.2**）

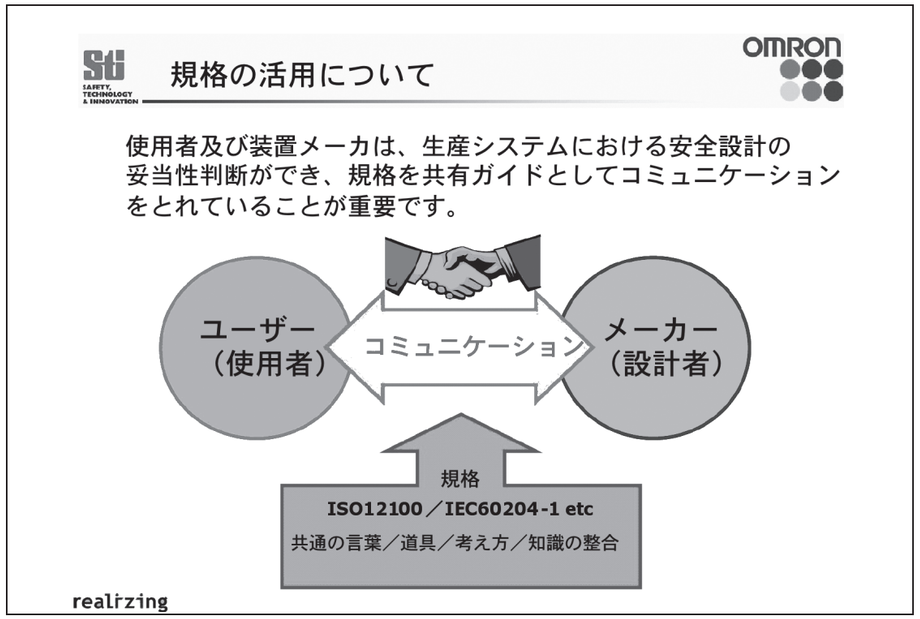


図1.8.2　労働災害防止の基本（出典 ： オムロン社資料）

（2）厚生労働省の指針について

厚生労働省の「改正労働安全衛生法」が平成１８年４月１日に施行され、それに伴い「機械の包括的な安全基準に関する指針」平成１９年７月３１日に改正された。

改正の概要は次の通りである。

1) 労働安全衛生法との関連が明確化

2) 機械メーカーのリスクアセスメントの手順明確化

3) 解説によりJISとの関連が明確化

など

改正された「機械の包括的な安全基準に関する指針」では、「機械の安全な使用」が出来るように、機械の製造等を行うものと機械のユーザー事業者の双方がリスクアセスメントの実施と保護方策の実施が求められている。（**図1.8.3**）

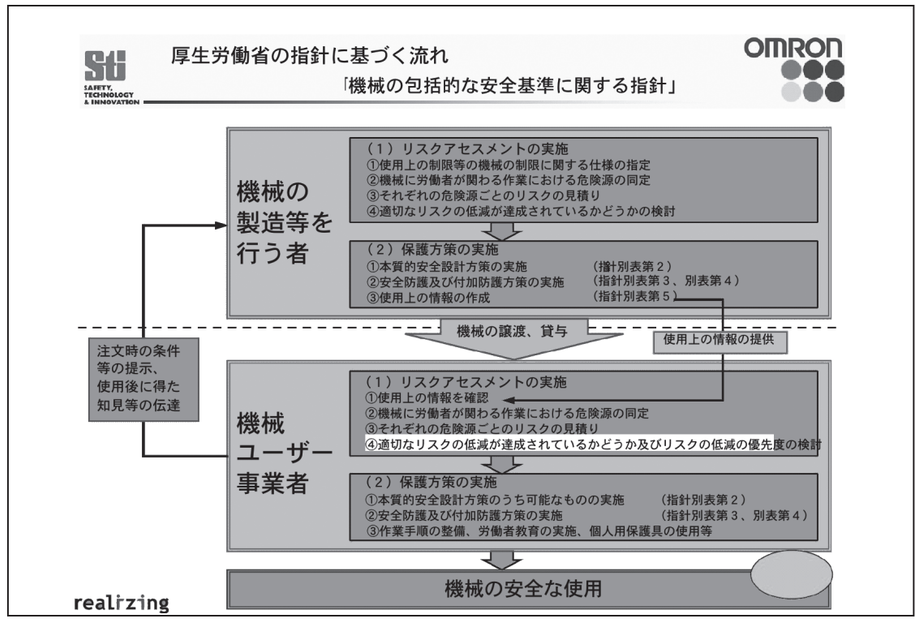


図1.8.3　厚生労働省の指針に基づく流れ（出典 ： オムロン社資料）

1.8.4　国際規格に基づく設計手順とリスクアセスメントについて

ここでは、リスクの評価をどのようにすすめ設計手順をどのように進め、安全に組み込むかを解説する。リスクアセスメントの詳細な解説は他の章を参照されたい。

リスクアセスメント

1）機械の使用状況範囲の決定

機械はその機械の使用が合理的に想定されるすべての状況において、安全であるように設計 ・ 製造されていなければならない。

「すべての状況」として考慮されるべき項目を次に上げる。

①機械のライフサイクルの各段階

製造、改造、運搬、流通、設置、調整、試運転、通常の使用、解体、廃棄

②目的用途

合理的に予見可能な誤使用、機能不良を含む

③作業者の身体的能力

視覚、聴覚などの五感の状態、体型、年齢、性別、利き手等

④機械従事者の訓練 ・ 経験レベル

熟練度、経験年数等

⑤合理的に予見可能な範囲において第三者が危険にさらされる可能性

部品補給、見学者等

2）危険源の同定－①

機械を使用するすべての状況（合理的に想定が可能なもの）における危険源、および危険状態を同定する

危険源（ハザード）の具体例

①物理的危険源

機械的 ・ 電気的 ・ 押しつぶし ・ 挟まれ ・ 騒音 ・ 熱的 ・ 騒音 ・ 放射線 ・ やけど ・ 放射線

②材料/物質による危険源

有害物質 ・ 刺激 ・ 粉塵 ・ 火災 ・ 爆発 ・ 生物など

③人間工学による危険源

不自然な姿勢 ・ 精神的過負荷 ・ 人間挙動など

④組合せによる危険源

個々には些細な危険源であっても、互いに組み合わされて重要顕著な危険源と同等になり得る

3）危険源の同定－②

「人は間違える」、「機械は壊れる」事を前提として危険源を同定しなければならない。

①人は間違える ： 作業経験によらず安全確保する。

②機械は壊れる ： 現場調整 ・ 保守時も安全確保する。

危険源に含まれるものの例を次に上げる。

①制御システムの故障/混乱

②動力源の故障

③電気設備に対する外部影響（電磁ノイズ、落雷等）

④ソフトウェアのエラー

⑤制御回路の故障

4）リスクの推定

リスクの推定は、次の「怪我の度合い ： S」、「危険にさらされる度合い ： F」、「危険を回避できる可能性 ： P」を元にリスクレベルを決定する。(ISO13849-1 ： 1999(JIS B 9705-1)

①怪我の度合い ： S

S１ ： 軽傷

S２ ： 重傷（手足の切断、死亡など）

②危険にさらされる度合い ： F

F１ ： まれに発生か短時間

F２ ： 頻繁あるいは常時か長時間

③危険を回避できる可能性 ： P

P１ ： 可能

P２ ： 逃げられない

5）リスクの評価

リスクの推定により得られたリスクレベルを元に、安全方策カテゴリ(B~4)を決定する。

(ISO13849-1 ： 1999(JIS B 9705-1)

安全方策カテゴリを決定する場合には、追加手段を併用したカテゴリを選択するか、余裕のある安全方策カテゴリを選択する

安全カテゴリの要旨を**図1.8.4**に上げる。

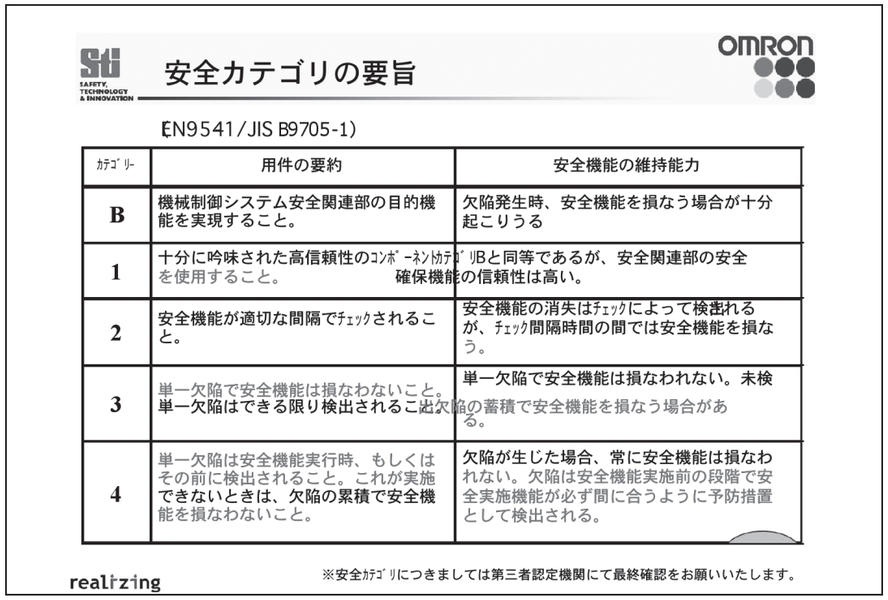


図1.8.4　安全カテゴリの要旨

6）設計手順

設計手順はISO 12100-2(JIS B9700-2)に基づく手順とし、選択した安全方策カテゴリを元にリスクを低減するためには本質安全設計をする事が重要であり、その一例を挙げる

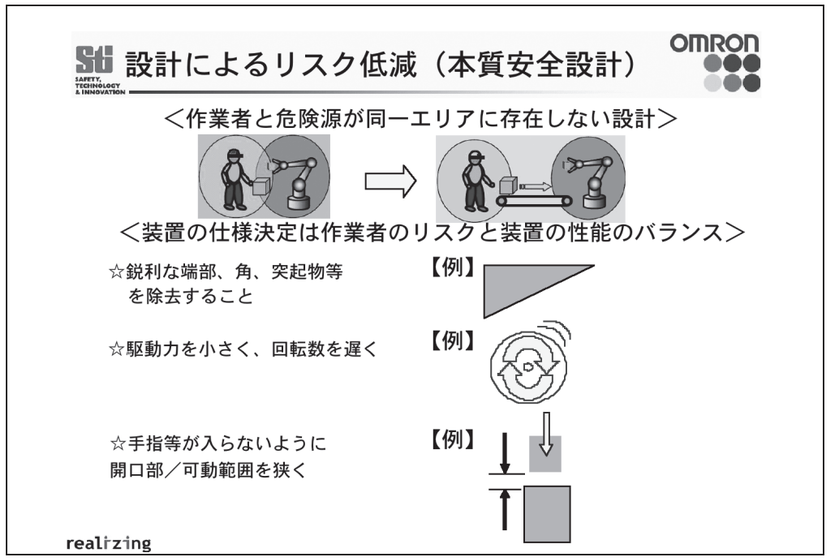


図1.8.5　厚生労働省の指針に基づく流れ（出典 ： オムロン社資料）

1.8.5　安全コンポーネントについて

安全コンポーネントは、次の要素を持ったものであり、これらを前提に設計する必要がある。

１）壊れない部品ではない。

２）あらゆる条件において危険な壊れ方をしない訳ではない。

３）一定の条件において、危険な壊れ方をしない、または壊れ方が定義されている

ポジションスイッチ（リミットスイッチ）、操作スイッチの故障除外事項を**表 1.8.1** に示す。（ ISO13849-2 付属書D）

表 1.8.1　ポジションスイッチ（リミットスイッチ）、操作スイッチの故障除外事項

考慮すべき故障	故障除外	備考
接点が閉じない	なし	
接点が開かない	IEC 60947 -5-1 付属書 K に適合した接点は開くと考えられる。	
互いに隔離されている隣接した接点間の短絡	IEC 60947 -5-1 に適合した接点の短絡は除外することができる。	ゆるんだ導電部が接点間の絶縁を橋絡するようなことがないのが望ましい。
切換接点の 3 つの端子間の同時短絡	IEC 60947 -5-1 に適合した接点の短絡は除外することができる。	
※機械的側面に関する故障については、付属書 A を参照する必要がある。		

（1）セーフティ ・ スイッチ

スイッチは、接点が溶着し過電流や経年変化のためスイッチの接点どうしが離れずＯＮしたままの状態になり、原理上１００％の防止はできない。

ノーマルクローズの接点を持つスイッチにする事で、直接開路動作機構が可能となる。

直接開路動作機構 ： 可動接点が非弾性素材の機械部品に連動して動き、たとえ接点が溶着しても一連の機構の直接的な力の伝達で、接点を強制的に開く機構。

（2）セーフティ ・ スイッチの種類

セーフティ ・ スイッチとして非常停止ボタン、セーフティ ・ ドアスイッチなどがあり、オムロン社の製品を**図 1.8.6** に示す。

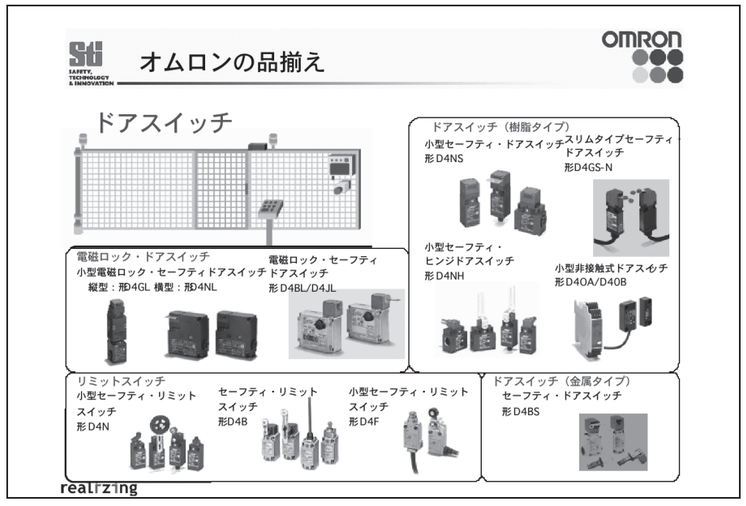


図 1.8.6　非常停止ボタン、セーフティ ・ ドアスイッチの製品（出典 ： オムロン社資料）

（3）イネーブルスイッチの種類

イネーブルスイッチは柵内などの危険領域において、作業者がスイッチを握っている時のみ機械が動作し、手を離したり強く握ったら、機械をOFFし、予期しない機械の動作から回避するために使用するもので、オムロン社の製品を**図 1.8.7** に示す。

図 1.8.7　イネーブルスイッチの製品（出典 ： オムロン社資料）

（4）セーフティ・ライトカーテン

安全が確認されたときだけ「ON」になり、故障、電源未投入、遮光（危険）時または、安全が確認できないときに「OFF」になるスイッチで、オムロン社の製品を**図1.8.8**に示す。

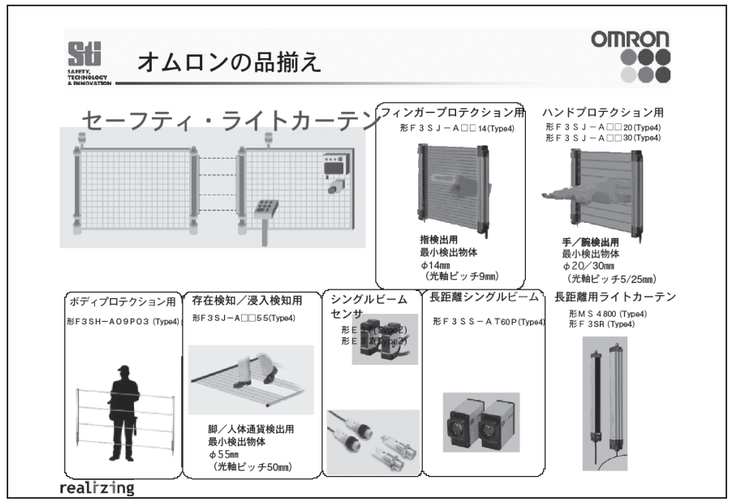


図1.8.8　セーフティ・ライトカーテンの製品（出典 ： オムロン社資料）

（5）存在検知用センサー

機械が作動する危険領域に人間がいる事を検知し、人間がいる場合は機械が動作しないようにする装置に使用するもので、圧力検知方式、透過光方式、反射光方式などのセンサーがある。オムロン社の製品を**図1.8.9**に示す。

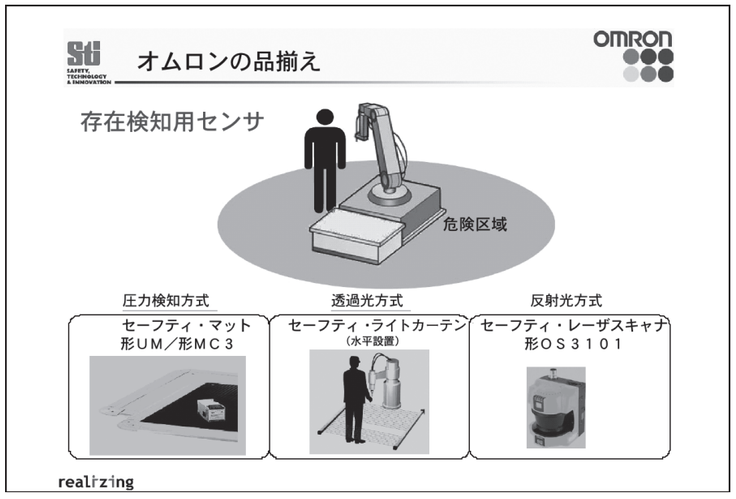


図1.8.9　存在検知センサーの製品（出典 ： オムロン社資料）

（6）セーフティ・リレー

セーフティ・スイッチのように強制的に引きはがす事は出来ないが、どのリレーが溶着したかが分かる安全回路に使用する事が出来る。
オムロン社の製品を**図1.8.10**に示す。

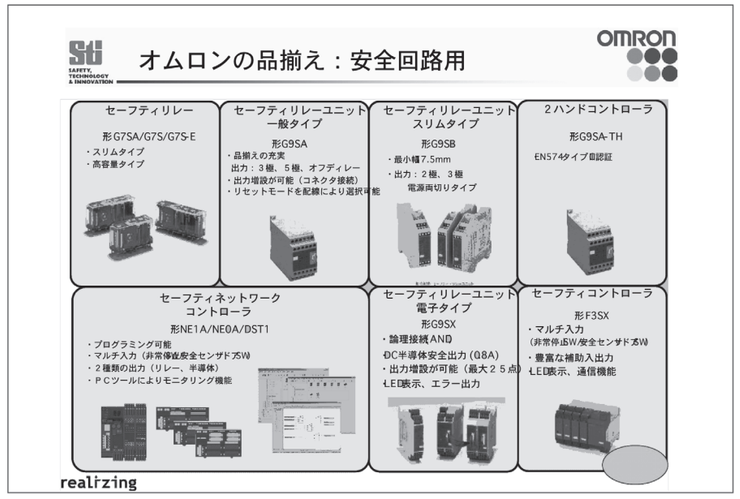


図1.8.10　安全回路用セーフティ・リレーの製品（SIL3認証製品を含む）
（出典 ： オムロン社資料

1.8.6　まとめ

機械安全設計手順は安全に関する国際規格に従う事が重要であり、安全コンポーネントを適切に使用する事で、安全装置、安全回路を構築できて労働災害に対する予防と防止の方策を講じる事が可能となる。

今後共に、技術の発展に伴い安全コンポーネント製品の機能と性能が向上する事を願う。

1.9　ＥＴ２０１０技術本部セミナー講演

本節は、2010年12月1日、ＥＴ２０１０初日に本ワーキングメンバーにて講演したセミナー内容をまとめたものである。

1.9.1　セミナー概要

セミナーは、３講師、計３時間弱の開催である。１５０人定員に対し、定員を超える事前申し込みがあり、当日も１２０席に対し、１３０名を越える参加者があり、昨日安全への関心は大きかった。アンケートも詳細後述にあるように好意的で、評価も高かった。セミナー内容は、おおよそ以下の内容である（詳細はプレゼン資料参照)。

開催場所　；　横浜パシフィコ
開催日時　；　２０１０年１２月　１日　14:30～17:30
題目　　；　ＥＴ２０１０／組込み総合技術展
　　併催セミナー 『ＪＡＳＡ技術本部セミナー』
　　「組み込みシステムの機能安全」
　　～　機能安全実現のために　～

講演者　　；　司会　入月康晴　（地独）東京都立産業技術研究センター
　　Ⅰ　金田光範　　東芝システムテクノロジー株式会社
　　Ⅱ　水口大知　（独）産業技術総合研究所
　　Ⅲ　兼本　茂　　会津大学　教授

講演概要　；

（Ⅰ）組込みシステムにおける安全設計

機能安全を理解するために、安全に関する主な用語や概念について解説した。また関連規格の動向、ソフトウェアの安全設計の考え方についても解説。

（Ⅱ）機能安全設計の基本

IEC 61508 に基づいて、安全度水準とその達成方法など、機能安全の基本的な考え方を解説。また、IEC 61508 Ed.2 の主要変更点も解説。

（Ⅲ）機能安全の将来動向と教育体系

欧米の技術動向、安全系の事例、ツールの紹介と会津大学で行っている機能安全教育の体系や講義の模様を解説。また、先月末米国で開催された学会からホットな話題も紹介。

1.9.2　聴講者アンケートの結果

１３３名の参加を頂き、アンケートの回収は１０４件。内容に不満を表明した回答は２件のみで、ほとんどが役に立ったという回答でありたいへん良好な結果であった。

具体的なコメントの内容では、今回はやや詰め込みすぎであるので、もう少しゆっくりと詳しい解説を希望する声が多かった。また、ISO 26262 の解説、A-SPICE　との関係、安全設計の実例などの希望も多かった。参加者は、ET2010の性格を反映してIT系企業が多いが、自動車系、機械系、計装制御系からも参加があった。また、職種では、開発部門とスタフが多く、品質管理系が少なかった。

これらは、次回開催する場合の参考にするとともに、委員会活動の方向付けにも参考としていきたい。

アンケートの詳細は、後述の表を参照方。

アンケートの詳細

技術本部セミナー 2010.12.1（安全性向上委員会　製品安全WG）

■事前登録出席　150名　　■当日出席　24名　　■合計　133名（内JASA会員31名）

	本展示会参加回数	Q1. 受講目的					Q2. 講演内容					Q3. 講演の仕方					Q4. 講演資料は？						Q5. 本講演についてのご感想	Q6. 今後希望されるセミナー	Q7. 展示会場には入場されましたか			Q8. その他、当協会、ET展に対して意見・ご要望等
		(1)技術情報収集	(2)業界動向調査	(3)研究調査	(4)係 CAの委員会関	(5)その他	(1)役に立った	(2)やや役にたった	(3)普通	(4)あまり役にたたなかった	(5)役に立たなかった	(1)大変良かった	(2)まあまあ良かった	(3)普通	(4)やや分かりにくかった	(5)分かりにくかった	(1)役にたった	(2)やや役に立った	(3)普通	(4)あまり役に立たなかった	(5)役に立たなかった				(1)入場した	(2)これから入場する	(3)入場しない	
	2.76	79	39	3	3	1	57	32	11	3	0	38	52	9	3	0	56	33	11	1	0		38	19	74	13	5	2
						125					103					102					101					92	
		63.2%	31.2%	2.4%	2.4%	0.8%	55.3%	31.1%	10.7%	2.9%	0.0%	37.3%	51.0%	8.8%	2.9%	0.0%	55.4%	32.7%	10.9%	1.0%	0.0%				80.4%	14.1%	5.4%	
1	3	○	○				○						○				○						機能安全の考え方、意識づけをどのように行えるか、兼本先生のお話が参考になりました。		○			
2	5				○		○					○					○								○			
3	7	○	○					○					○				○						兼本先生の講演は産業界の視点、アカデミックな視点など様々な視点で将来も見据えた取り組みを紹介頂き、大変興味深かった。			○		
4	5		○					○					○					○							○			
5	2	○					○						○				○								○			
6	1	○					○						○					○							○			
7	1		○				○					○					○						様々な面から機能安全規格のアウトラインを知ることが出来ました。	同様に機能安全に関するセミナーを要望しますが、医療系など他の機能安全規格についてもセミナーをお願いしたい。	○			
8	記載なし	○						○					○					○							○			
9	2	○						○				○						○								○		
10	1	○					○						○				○						機能安全の考え方を知ることができた。		○			
11	3	○	○					○					○					○							○			
12	1	○					○						○				○								○			
13	1		○					○					○					○							○			
14	1	○						○					○					○							○			
15	1	○							○				○					○					浅く広くの感があり、基本を知るには良い機会だった。もう少し掘り下げた説明も欲しかった。		○			
16	1	○						○					○				○						良く理解することができた		○			
17	3		○					○					○				○								○			
18	7		○				○					○					○											
19	1	○					○					○					○						大変勉強になりました。	機能安全の各社の事例紹介	○			
20	1	○						○					○					○							○			
21	1	○					○					○					○						社会のインフラ部分でも多くの組込みシステムが使用されている。またシステムも複雑になっている。安全性は最も重要なテーマと思う。	・ 安全設計手法 ・ 本質を絞りこんだ規格について			○	
22	1	○							○					○				○					もう少しゆっくりと。中身が濃いので、略した部分が相当あった。	今回のテーマを再度お願いしたい	○			
23	5	○					○						○				○								○			
24	3	○						○					○				○								○			
25	記載なし	○	○				○						○				○								○			
26	2					業界のレベル調査				○				○				○					1部間違いもあり、もう少し正確さを要求したい	日本では61508がメインになりすぎており、それ以外の安全への対応へのセミナーがあると良い		○		
27	3	○	○					○				○					○								○			
28	5		○				○					○					○						安全に関して規格および原則、原理、理想等考えさせられた。		○			
29	4	○						○					○					○							○			
30	10	○	○					○					○					○										
31	1		○				○					○						○					安全の考え方の基本を理解できました。今後は具体的製品で考えを深めていきたい。		○			
32	2	○					○					○						○					ボリュームが多く、かけ足な内容だったのが、残念だった。	ISO26262のテクニカルなセミナー	○			
33	1		○				○						○						○						○			
34	3			○				○					○					○							○			
35	3	○					○					○					○								○			
36	1	○						○					○										大変勉強になった。説明もわかりやすかった。特に「機能安全設計の基本」が良かった。配布資料も充実しており良かった。	引き続き組込みシステムの機能安全の事例紹介やそれに使用できる手法の技術的話をききたい。			○	

	本展示会参加回数	Q1．受講目的					Q2．講演内容					Q3．講演の仕方					Q4．講演資料は？						Q5．本講演についてのご感想	Q6．今後希望されるセミナー	Q7．展示会場には入場されましたか			Q8．その他、当協会、ET展に対して意見・ご要望等
		(1)技術情報収集	(2)業界動向調査	(3)研究調査	(4)CASA委員会関係	(5)その他	(1)役に立った	(2)やや役にたった	(3)普通	(4)あまり役にたたなかった	(5)役に立たなかった	(1)大変良かった	(2)まあまあ良かった	(3)普通	(4)やや分かりにくかった	(5)分かりにくかった	(1)役にたった	(2)やや役に立った	(3)普通	(4)あまり役に立たなかった	(5)役に立たなかった				(1)入場した	(2)これから入場する	(3)入場しない	
	2.76	79	39	3	3	1	57	32	11	3	0	38	52	9	3	0	56	33	11	1	0		38	19	74	13	5	2
						125					103					102					101					92	
		63.2%	31.2%	2.4%	2.4%	0.8%	55.3%	31.1%	10.7%	2.9%	0.0%	37.3%	51.0%	8.8%	2.9%	0.0%	55.4%	32.7%	10.9%	1.0%	0.0%				80.4%	14.1%	5.4%	
37	2	○	○				○					○					○						各産業分野毎の日本の持つ知見が、どうIEC61508を中心に集められ、かつ本文やでの日本のプレセンスを発揮できるようになるかが今後の課題だと感じました。		○			
38	5	○	○				○						○				○								○			
39	6		○				○					○					○						安全に関する基本的な考え方から解説されたのは良かった。	実例を中心としたものが有効かと思います。				
40	3	○					○					○					○								○			
41	1	○	○				○						○					○							○			
42	3	○					○					○					○								○			
43	4	○					○					○					○								○			
44	5	○					○					○					○						兼本先生の講演が非常に分かりやすく、興味をもつ内容だった。		○			
45	1	○					○					○					○								○			
46	1	○	○					○				○					○						PPTマスキングは文字つぶれの無いような選色とすべき。		○			展示会会場とセミナー会場（会議センター）が遠すぎる。同一ビル内でできないか？
47	3	○					○					○					○						兼本先生の講演は具体的なものが多く面白かった。		○			
48	1		○				○						○					○							○			
49	1	○					○					○					○						複雑なIEC61508の概要を理解することが出来た。		○			
50	1				○			○				○						○							○			
51	1	○					○						○				○								○			
52	記載なし	○	○				○						○					○							○			
53	1	○							○					○					○						○			
54	記載なし	○	○				○					○					○									○		
55	記載なし	○					○						○				○								○			
56	8	○						○					○				○									○		
57	8	○	○				○					○					○									○		
58	2	○	○				○						○					○							○			
59	8	○					○						○				○						機能安全について今まで以上に理解を深めることができた。		○			
60	1	○					○					○					○							ISO26262の紹介				
61	1	○	○				○								○				○				●「Ⅲ．機能安全設計の基本」は時間の割に内容盛り沢山で消化不良。TFMなど算出の具体例が欲しかった。●「Ⅳ．機能安全の将来動向と教育体系」は非常に参考になりました。	抽象化（モデリング）教育（社会人向け）		○		
62	1	○						○					○					○							○			
63	2	○	○					○					○					○					IEC61508とISO26262について今回のセミナーで知る機会ができて良かった。ISOの監査では9001だけではなく、26262も視野に入れていきたいと思った。	世界で広まっている規格や認証機関などを紹介するような内容のセミナー	○			
64	1		○				○						○				○								○			
65	2	○					○						○				○						内容に対して時間が足りなく感じた。同内容に2倍の時間をかけても良いと思う	ISO26262	○			
66	1	○					○						○					○					基本的な部分についての話もあり、初めての参加でもある程度の理解できた為、有意義でした。IEC61508についてはかなり学習が必要かと感じました。				○	今後もセミナーの情報をチェックして参加したい
67	5	○	○					○					○					○										
68	3	○							○					○					○						○			
69	1		○					○				○							○					ISO26262	○			
70	3	○																					講演の進行がはやかったので、もう少しゆっくり細かく説明していただけるとより良かった。		○			
71	2	○					○						○					○					水口氏の講演は大変参考になった。		○			
72	1	○						○						○				○					IEC61508やSILについての定義、理解があいまいだったので、聞けて良かった。	安全システムについてのセミナー	○			

	本展示会参加回数	Q1．受講目的					Q2．講演内容					Q3．講演の仕方					Q4．講演資料は？						Q5．本講演についてのご感想	Q6．今後希望されるセミナー	Q7．展示会場には入場されましたか			Q8．その他、当協会、ET展に対して意見・ご要望等
		(1)技術情報収集	(2)業界動向調査	(3)研究調査	(4)CASA委員会関係	(5)その他	(1)役に立った	(2)やや役にたった	(3)普通	(4)あまり役にたたなかった	(5)役に立たなかった	(1)大変良かった	(2)まあまあ良かった	(3)普通	(4)やや分かりにくかった	(5)分かりにくかった	(1)役にたった	(2)やや役に立った	(3)普通	(4)あまり役に立たなかった	(5)役に立たなかった				(1)入場した	(2)これから入場する	(3)入場しない	
	2.76	79	39	3	3	1	57	32	11	3	0	38	52	9	3	0	56	33	11	1	0		38	19	74	13	5	2
						125					103					102					101					92	
		63.2%	31.2%	2.4%	2.4%	0.8%	55.3%	31.1%	10.7%	2.9%	0.0%	37.3%	51.0%	8.8%	2.9%	0.0%	55.4%	32.7%	10.9%	1.0%	0.0%				80.4%	14.1%	5.4%	
73	7			○			○					○					○								○			
74	4		○				○					○					○								○			
75	記載なし	○	○						○				○						○				知見が広まった。		○			
76	3	○						○					○					○						Automotive SPICEと機能安全をからめたセミナー	○			
77	10	○							○					○					○					Automotiveにおいての機能安全の実装について	○			
78	1	○	○				○					○					○						●水口氏の割愛した部分も聞きたかった。●もう少し26262の話もあれば●音響のせいか聞きづらいところもあった	ISO26262とAuto- motive SPICE			○	
79	1	○						○				○					○								○			
80	2	○					○					○					○						とてもわかりやすいセミナーと思います。			○		
81	1		○				○					○					○									○		
82	2	○							○				○						○								○	
83	2	○					○						○				○							ISO26262の規格に対するセミナー				
84	1		○						○										○						○			
85	2	○					○						○				○											
86	5	○						○				○						○								○		
87	4	○					○						○				○								○			
88	3		○					○				○					○								○			
89	1	○	○				○					○					○						参考資料はすでに読んでいたので、内容は理解していたが、機能安全の将来動向と教育体系の話は興味深く面白かった。		○			
90	5	○						○					○					○							○			
91	記載なし		○					○					○					○					安全の定義をもう少し詳しくお願いしたい		○			
92	1	○					○					○					○											
93	3	○							○					○					○									
94	1		○						○					○					○							○		
95	記載なし	○					○						○					○					略語が多い。補足説明を記載してほしい					
96	1	○					○						○				○								○			
97	5	○	○					○					○					○					無料のセミナーでここまで聞けるとは思いませんでした。規格法制化の本質を見極めて、製品安全にフォーカスすべきと改めて思いました。	ISO26262		○		
98	記載なし	○					○						○				○						資料もわかりやすかった		○			
99	記載なし	○							○				○				○								○			
100	記載なし			○	○		○					○					○											
101	記載なし	○					○					○					○											
102	記載なし									○					○					○			仕事に役立つ具体性がない		○			
103	記載なし	○						○						○			○								○			
104	記載なし	○								○					○								手法とかではなく、事例をふまえた講義をしていただきたかった。			○		

ET2010製品安全WGセミナーアンケート分析結果

2011/1/21　SA-WG

No	Q5. 本講演についてのご感想	Q6. 今後希望されるセミナー		関心先			今後の期待セミナー					WG活動反映事項				備考
				Ⅱ	Ⅲ	Ⅳ	26262	事例紹介	技法実例	規格認証	その他	新テーマ	深堀	プレゼン	その他	
	38	19														
1	機能安全の考え方、意識づけをどのように行えるか、兼本先生のお話が参考になりました。					1										
2	兼本先生の講演は産業界の視点、アカデミックな視点など様々な視点で将来も見据えた取り組みを紹介頂き、大変興味深かった。					1										
3	様々な面から機能安全規格のアウトラインを知ることが出来ました。	同様に機能安全に関するセミナーを要望しますが、医療系など他の機能安全規格についてもセミナーをお願いしたい。		1	1	1		1								
4	機能安全の考え方を知ることができた。			1	1	1										
5	浅く広くの感があり、基本を知るには良い機会だった。もう少し掘り下げた説明も欲しかった。			1	1	1										
6	良く理解することができた			1	1	1										
7	大変勉強になりました。	機能安全の各社の事例紹介		1	1	1		1								
8	社会のインフラ部分でも多くの組込みシステムが使用されている。またシステムも複雑になっている。安全性は最も重要なテーマと思う。	・安全設計手法 ・本質を絞りこんだ規格について		1	1	1			1	1			1			
9	もう少しゆっくりと。中身が濃いので、略した部分が相当あった。	今回のテーマを再度お願いしたい		1	1	1								1		
10	1部間違いもあり、もう少し正確さを要求したい	日本では61508がメインになりすぎており、それ以外の安全への対応へのセミナーがあると良い								1		1			1	
11	安全に関して規格および原則、原理、理想等考えさせられた。			1	1	1										
12	安全の考え方の基本を理解できました。今後は具体的製品で考えを深めていきたい。			1	1	1										
13	ボリュームが多く、かけ足な内容だったのが、残念だった。	ISO26262のテクニカルなセミナー		1	1	1	1							1		
14	大変勉強になった。説明もわかりやすかった。特に「機能安全設計の基本」が良かった。配布資料も充実しており良かった。	引き続き組込みシステムの機能安全の事例紹介やそれに使用できる手法の技術的話をききたい。		1	2	1		1	1							
15	各産業分野毎の日本の持つ知見が、どうIEC61508を中心に集められ、かつ本文やでの日本のプレセンスを発揮できるようになるかが今後の課題だと感じました。			1	1	1										
16	安全に関する基本的な考え方から解説されたのは良かった。	実例を中心としたものが有効かと思います。		1	1	1			1				1			
17	兼本先生の講演が非常に分かりやすく、興味をもつ内容だった。					1										
18	PPTマスキングは文字つぶれの無いような選色とすべき。													1		
19	兼本先生の講演は具体的なものが多く面白かった。					1										
20	複雑なIEC61508の概要を理解することが出来た。			1	1	1										
21	機能安全について今まで以上に理解を深めることができた。			1	1	1										

No	Q5. 本講演についてのご感想	Q6. 今後希望されるセミナー		関心先			今後の期待セミナー					WG活動反映事項				備考
				Ⅱ	Ⅲ	Ⅳ	26262	事例紹介	技法実例	規格認証	その他	新テーマ	深堀	プレゼン	その他	
22		ISO26262の紹介					1									
23	●「Ⅲ. 機能安全設計の基本」は時間の割に内容盛り沢山で消化不良。TFMなど算出の具体例が欲しかった。●「Ⅳ. 機能安全の将来動向と教育体系」は非常に参考になりました。	抽象化（モデリング）教育（社会人向け）				1							1			
24	IEC61508とISO26262について今回のセミナーで知る機会ができて良かった。ISOの監査では9001だけではなく、26262も視野に入れていきたいと思った。	世界で広まっている規格や認証機関などを紹介するような内容のセミナー		1	1	1				1						
25	内容に対して時間が足りなく感じた。同内容に2倍の時間をかけても良いと思う	ISO26262		1	1	1	1							1		
26	基本的な部分についての話もあり、初ての参加でもある程度の理解できた為有意義でした。IEC61508についてはかなり学習が必要かと感じました。			1	1	1										
27		ISO26262					1									
28	講演の進行がはやかったので、もう少しゆっくり細かく説明していただけるとより良かった。													1		
29	水口氏の講演は大変参考になった。				1											
30	IEC61508やSILについての定義、理解があいまいだったので、聞けて良かった。	安全システムについてのセミナー		1	1	1		1	1				1			
31	知見が広まった。			1	1	1										
32		Automotive SPICEと機能安全を絡めたセミナー								1	1	1				
33		Automotiveにおける機能安全実装について								1	1	1				
34	●水口氏の割愛した部分も聞きたかった。●もう少し26262の話もあれば●音響のせいか聞きづらいところもあった	ISO26262とAuto- motive SPICE			1		1				1	1		1		
35	とてもわかりやすいセミナーと思います。			1	1	1										
36		ISO26262の規格に対するセミナー					1									
37	参考資料はすでに読んでいたので、内容は理解していたが、機能安全の将来動向と教育体系の話は興味深く面白かった。			1	1	2										
38	安全の定義をもう少し詳しくお願いしたい												1			
39	略語が多い。補足説明を記載してほしい													1		
40	無料のセミナーでここまで聞けるとは思いませんでした。規格法制化の本質を見極めて、製品安全にフォーカスすべきと改めて思いました。	ISO26262		1	1	1	1									
41	資料もわかりやすかった			1	1	1										
42	仕事に役立つ具体性がない			−1	−1	−1										
43	手法とかではなく、事例をふまえた講義をしていただきたかった。							1	1					1		
				23	26	29	7	5	5	5	3	4	5	8	1	

1. 今後のセミナーへの期待について ： ISO 26262の紹介 ・ 解説、事例や技法実例の紹介、
   A-SPICEno解説、の希望がある。但しプレゼンは絞りこんだほうがよさそう。
2. WG活動への反映事項について ： ①IEC 61508だけでなく、A-SPICE、ISO 26262まで、拡げるかどうか。②安全システムの設計技法という切り口が考えられる。③啓発活動
3. プレゼン資料の工夫も必要。

製品安全WG企画　ET2010セミナー　の結果

2011/1/21

来場者分析

業種別		
メーカー系	自動車	14
	JEMIMA系	8
	電機	33
	電機（TST）	16
	その他	39
非メーカー系	自治体 ・ 教育	5
	その他	15
その他		3
		133

＊

職種別（部門別）	
研究所 ・ 開発C	29
設計 ・ ソフト開発	48
品質管理	5
スタフ ・ その他	47

＊ ···· H; 7、F ： 3、N ： 3、P ： 8、T: 12

見解

１．テーマからみても、組込み系に係っている方々が多く参加している。

２．Ｔ社系は、講師の出身なので、参加者が多い。よってこれを除くと、P社系とH社系が多く参加している。M社系が全くいないのも興味深い。なお、機能安全のノウハウを社内に広く保有する企業は、M、H、T、及び石化エンジニアリング会社と宇宙航空関係と思われる。

３．職種別では、スタフ系が比較的多く、品質管理系が少ない（と思われる）。

第２章
機能安全関連製品調査

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に関連している製品の現状を調査した。前年度と同様にシステム又はソフトウェアを構成するコンポーネント、並びに開発を支援するツールに分けて調査を行った。

表2.1　調査方法の概要

調査期間	2010 年 4 月から 2011 年 2 月。
調査対象	ET2010 等の展示会、ネット検索等を利用して抽出した。なお、既に認証を取得しているものだけでなく、今後、認証取得を予定している製品、又は認証取得を支援する製品も含めた。
調査票の作成	製品カタログ、ホームページに公開されている資料等を参照し、一部、販売元の協力を得て調査票を作成。

０９年度調査製品　：　番号1～１６

１０年度調査製品　：　番号１７～２２

表2.2　SIL3取得関連製品一覧

番号	開発元/販売元	製品名	製品区分
1	Green Hills Software/ アドバンスドデータコントロールズ	INTEGRITY	RTOS
2	ETAS/ イータス	ASCET	コード生成
3	Wind River/ ウィンドリバー	VxWorks	RTOS
4	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
5	オムロン	フレキシブルセーフティユニットG9SX	PLC
6	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
7	キーエンス	セーフティコントローラＳＣシリーズ	PLC
8	光洋電子工業	KOSTAC　Safety　AZ-C1	PLC
9	サンクス	小型ビームセンサST4	光センサ
10	Esterel Technologies/ シーディアダプコジャパン	SCADE　Suite	コード生成
11	ジェイテクト(JTEKT)	TOYOPUC-PCS	PLC
12	東芝システムテクノロジー	安診太郎	安全性評価
13	日本AS-i協会会員	AS-Interface Safety at Work	ネットワーク
14	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
15	三菱電機	安全シーケンサMELSEC　safety	PLC
16	Rockwell Automation/ ロックウェルオートメーションジャパン	GuardPLCシステム	PLC
17	ＫＩＴＺ	緊急遮断用アクチュエータ（ＨＡＳ型）	アクチュエータ
18	QNXソフトウェアシステムズ	QNX Neutrino RTOS セーフカーネル	RTOS
19	SCIOPTA(スキオプタ)システム(スイス)	SCIOPTA ARM IEC 61508-P3	RTOS
20	オムロン	セーフティネットコントローラG9SP	PLC
21	MKS INTEGRITY　株式会社	MKS　INTEGRITY	認証支援
22	PARASOFT CORPORATION	C++test7.3.2	認証支援

SIL3関連製品調査票(1)

種別		ソフトウェアコンポーネント	
製品名		INTEGRITY	
製品区分		RTOS	
特徴	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を分離。 ● タスクごとにメモリとプロセサ時間の割当てを保証。 ● 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、μITRON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、最新のモデルベース開発ツールとの協調連携が可能。	
	動作条件/ 動作環境	● ハードウェアによるメモリ保護機構が必要。 ● X86、ARM、OMAP等のアーキテクチャをサポート。	
規格	適合規格	SIL3	DO-178B(レベルA)
	取得時期	2006年6月	
	認定機関	TUV	
開発元		米国Green Hills Software http://www.ghs.com/	
販売	販売元	アドバンスドデータコントロールズ http://www.adac.co.jp/	
	価格		
	販売時期	販売中	
	製品情報	http://www.adac.co.jp/products/integrity/details/page01.html	
利用ガイド		● 航空宇宙、防衛等の分野で使用されていて、強いリアルタイム性を必要とするFA分野等に利用可能。 ● SIL の異なるアプリケーションが混在するとき、それらを分離して相互干渉を防止するために使うことができる。 ● SCADEとの連携が可能である。 ● 認証取得のためのコンサルティングや支援サービスを利用できる(提供はExida社)。	

SIL3関連製品調査票(2)

種別		ツール
製品名		ASCET
製品区分		コード生成
特徴	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。
	動作条件/動作環境	
規格	適合規格	SIL3
	取得時期	
	認定機関	TUV
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	販売元	イータス http://www.etas.com/ja/index.php
	価格	
	販売時期	販売中
	製品情報	http://www.etas.com/ja/products/ascet_software_products.php
利用ガイド		● 1997 年のリリース以来、生成されたコードは数千万もの量産用 ECU で使用されている。 ● 車載用のソフトウェアの開発、あるいはモデルベース開発を行うときに利用できるツールである。

SIL3関連製品調査票(3)

種別		ソフトウェアコンポーネント	
製品名		VxWorks	
製品区分		RTOS	
特徴	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。	
	動作条件/動作環境		
規格	適合規格	SIL3(認証可能)	DO-178B(レベル A、認証可能)
	取得時期		
	認定機関		
開発元		Wind River(米国) http://www.windriver.com/	
販売	販売元	ウィンドリバー http://www.windriver.com/japan/	
	価格		
	販売時期	販売中	
	製品情報	http://www.windriver.com/japan/products/vxworks/index.html	
利用ガイド		認証取得を支援するために、Wind River Platform for Safety Critical というソリューションを提供している。その概要は図 8.2 を参照。	

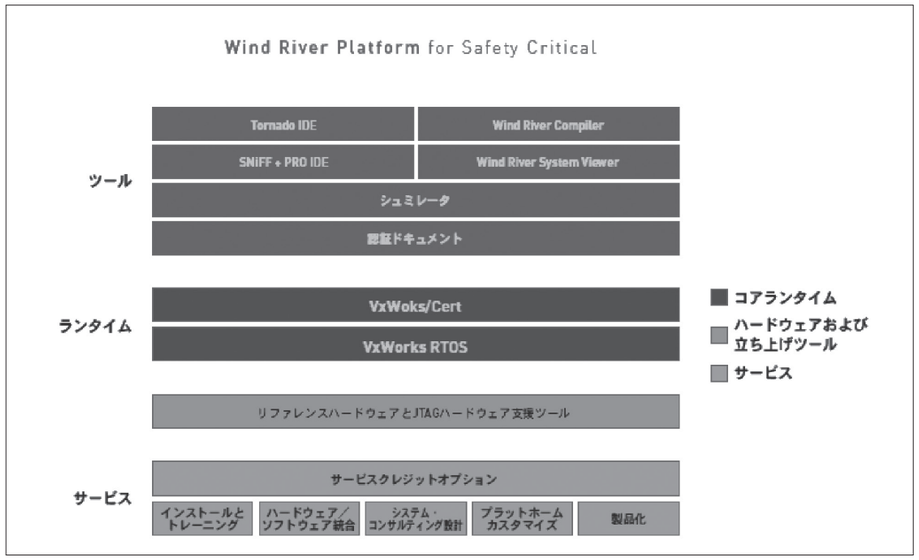


図8.2　認証可能なCOTSソリューションの体系図

SIL3関連製品調査票(4)

種別		システムコンポーネント	
製品名		セーフティネットワークコントローラ NE1A-SCPU シリーズ	
製品区分		PLC	
特徴	主要機能	● 従来、リレーを組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ブロックを選択、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。	
	動作条件/動作環境	ネットワークとして DeviceNet を使用できる。	
規格	適合規格	SIL3	ISO13849-1(カテゴリ 4)
	取得時期		
	認定機関	TUV	
開発元		オムロン http://www.omron.co.jp/r_d/index.html	
販売	販売元	オムロン http://www.fa.omron.co.jp/index.html	
	価格	ネットワークコントローラ NE1A-SCPU01-V1:　20 万円 I/O ターミナル DST1-ID12SL-1:　9 万円	
	販売時期	販売中	
	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	
利用ガイド		リレーで構成していた安全制御回路を PLC に置き換え、かつ、マルチベンダネットワーク DeviceNet での接続を実現できる。	

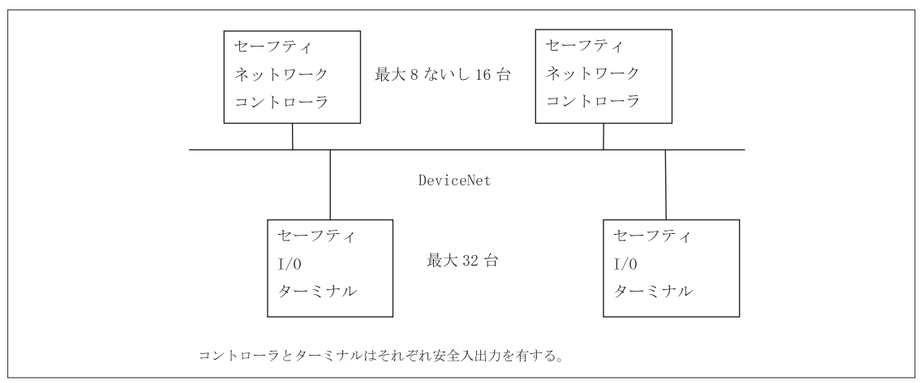


図8.3　DeviceNet Safetyシステムの構成図

SIL3関連製品調査票(5)

種別		システムコンポーネント	
製品名		フレキシブル　セーフティユニット G9SX	
製品区分		PLC	
特徴	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。	
	動作条件/動作環境		
規格	適合規格	SIL3	ISO13849-1(カテゴリ 4)
	取得時期		
	認定機関	TUV	
開発元		オムロン http://www.omron.co.jp/r_d/index.html	
販売	販売元	オムロン http://www.fa.omron.co.jp/index.html	
	価格	G9SX-AD322-T15-RT: 47,000 円	
	リリース時期	販売中	
	製品情報	http://www.fa.omron.co.jp/product/family/1524/index_p.html	
利用ガイド		装置をユニットごとに停止させたり、装置の構成変更が多い安全制御回路に適用できる。	

SIL3関連製品調査票(6)

種別		システムコンポーネント	
製品名		セーフティ　ライトカーテン SL-V シリーズ	
製品区分		ライトカーテン	
特徴	主要機能	● 機器の存在が見える表示灯内蔵。 ● 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。	
	動作条件/ 動作環境	● スリムタイプ保護構造 IP65 ● 堅牢・防水タイプ IP67/65	
規格	適合規格	SIL3	ISO13849-1(カテゴリ 4、PLe)
	取得時期	2007 年 3 月	同左
	認定機関	TUV	同左
開発元		キーエンス http://www.keyence.co.jp/index.jsp	
販売	販売元	キーエンス	
	価格	65,000 円から	
	販売時期	2007 年 3 月から販売	
	製品情報	http://www.keyence.co.jp/switch/safety/sl_v/index.jsp	
利用ガイド		危険区域への侵入検知に利用。	

SIL3関連製品調査票(7)

種別		システムコンポーネント	
製品名		セーフティコントローラ SC シリーズ	
製品区分		PLC	
特徴	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。	
	動作条件/ 動作環境	保護構造 IP20（制御盤内での使用）	
規格	適合規格	SIL3	ISO13849-1(カテゴリ 4、PLe)
	取得時期	2007 年 8 月	同左
	認定機関	TUV UL	同左
開発元		キーエンス http://www.keyence.co.jp/index.jsp	
販売	販売元	キーエンス	
	価格	28,000 円から	
	販売時期	2007 年 8 月から販売	
	製品情報	http://www.keyence.co.jp/switch/safety/sl_v/index.jsp	
利用ガイド		安全機器制御実施時に利用。	

SIL3関連製品調査票(8)

種別		システムコンポーネント	
製品名		KOSTAC　Safety　AZ-C1	
製品区分		PLC	
特徴	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-回路チェック機能	
	動作条件/動作環境	● 電源　DC24V　2A ● 周囲温度　0-55 ℃ ● 相対湿度　30-85% RH(但し結露なきこと)	
規格	適合規格	SIL3	IS013849-1(PLe)
	取得時期	2008 年	同左
	認定機関	TUV BGIA（ドイツ労働安全技術研究所）	
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	販売元	光洋電子工業 http://www.koyoele.co.jp/	
	価格		
	販売時期	2009 年 3 月販売開始予定	
	製品情報	問い合せ先は次の通り： 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　042-345-7994 mail　info@koyoele.co.jp	
利用ガイド		● 従来の安全制御回路のプログラム化を実現。 ● ファンクションブロック機能による安全回路の標準化。	

SIL3関連製品調査票(9)

種別		システムコンポーネント	
製品名		小型ビームセンサ ST4	
製品区分		光センサ	
特徴	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 コントローラに最大 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。	
	動作条件/動作環境		
規格	適合規格	SIL3	IS013849-1(カテゴリ 4、PLe)
	取得時期		
	認定機関		
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	販売元	サンクス http://sunx.jp/index.html	
	価格	● センサヘッド:　19,800 円から ● コントローラ:　39,800 円から	
	販売時期	販売中	
	製品情報	http://sunx.jp/japanese/products/safety/st4/index.html	
利用ガイド		危険区域における侵入検知に利用する。	

SIL3関連製品調査票(10)

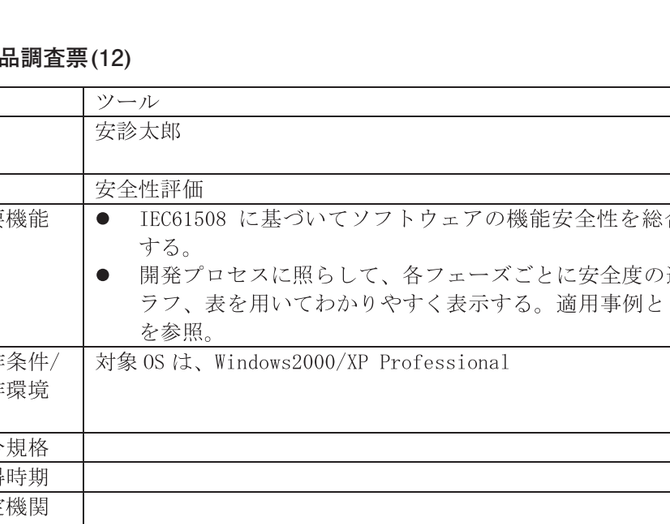
種別		ツール	
製品名		SCADE Suite	
製品区分		コード生成	
特徴	主要機能	● 要件管理機能によるトレーサビリティ管理 ● システム設計ツールとのインターフェース(SysML/UML、アルゴリズム設計ツール) ● SCADE 言語によるモデリング(データフロー/制御フローの自由な構造) ● モデルレベルでの検証支援(セマンティックチェック、モデルシミュレーション、モデルカバレッジ、形式検証、ワーストケース実行時間見積り、コンパイラ検証キット) ● 認証可能なCコードの自動生成 ● 設計モデルに対するレポートの自動生成	
	動作条件/動作環境	対象OSは、Windows XP、Windows VISTA	
規格	適合規格	SIL3/ EN-50128(SIL4)	DO-178B(レベルA)
	取得時期	2008年11月(SCADE6.0版)	製品版ごとで認証取得
	認定機関	TUV	
開発元		Esterel Technologies(フランス) http://www.esterel-technologies.com/	
販売	販売元	シーディー・アダプコ・ジャパン http:://www.cdaj.co.jp/	
	価格	450万～ (モジュール構成で価格は変わる)	
	販売時期	販売中	
	製品情報	http://www.cdaj.co.jp/product/070000scade/index.html	
利用ガイド		● 要件管理からソフトウェア設計、検証、自動コード生成、ドキュメント生成までの工程を1ツール環境でサポートできる。 ● 民間航空・宇宙・防衛の分野で主に使用されていて、DO-178B レベルA認証プロジェクトでの適用実績あり。IEC-61508/EN-50128認証プロジェクトにも適用中。 ● 生成コードは、MISRA-C準拠、ANSI-C準拠。 ● RTOS(INTEGROTY、VxWorks)統合コード生成可能。 ● 認証取得のためのコンサルティングや支援サービスを利用できる(各規格に対するハンドブック提供)。	

SIL3関連製品調査票(11)

種別		システムコンポーネント	
製品名		TOYOPUC-PCS	
製品区分		PLC	
特徴	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用I/F 別途ゲートウェイモジュール必要) ● 安全ラダー回路チェック機能	
	動作条件/動作環境	● 電源 DC24V 2.5A ● 周囲温度 0-50 ℃ ● 相対湿度 30-85% RH(但し結露なきこと)	
規格	適合規格	SIL3	IS013849-1(PLe)
	取得時期	2004年	同左
	認定機関	TUV BGIA (ドイツ労働安全技術研究所)	
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	販売元	ジェイテクト	
	価格	営業に問い合せ(0566-25-5140)	
	販売時期	販売中	
	製品情報	http://www.jtekt.co.jp/products/toyopuc/toyopuc-pcs/index.htm	
利用ガイド		● 従来の安全制御回路のプログラム化を実現。 ● ファンクションブロック機能による安全回路のスリム化および標準化。 ● 安全フィールドバス機能による大規模システム対応。	

SIL3関連製品調査票(12)

種別		ツール
製品名		安診太郎
製品区分		安全性評価
特徴	主要機能	● IEC61508 に基づいてソフトウェアの機能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。
	動作条件/動作環境	対象 OS は、Windows2000/XP Professional
規格	適合規格	
	取得時期	
	認定機関	
開発元		東芝システムテクノロジー http://www3.toshiba.co.jp/tst/
販売	販売元	東芝システムテクノロジー
	価格	
	販売時期	販売中
	製品情報	http://www3.toshiba.co.jp/tst/product/anshintaro.htm
利用ガイド		● 現状の開発プロセス、開発技術力を評価し、目標とする安全度水準との差異を分析するために利用する。 ● ツールに関するコンサルティングも利用可能。

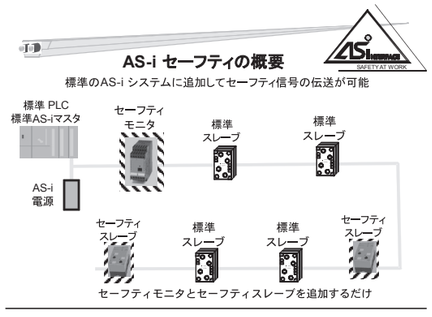


出典:東芝システムテクノロジーの製品カタログから引用

図8.4　安診太郎の適用事例

SIL3関連製品調査票(13)

種別		システムコンポーネント	
製品名		AS-Interface Safety at Work	
製品区分		ネットワーク	
特徴	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を可能とする。 ● 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サー、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。	
	動作条件/動作環境	● ﾄﾎﾟﾛｼﾞｰ　；トリー、ライン、スターの配線 ● 使用電線；２線式配線で電源と信号を重畳	
規格	適合規格	SIL3	IS013849-1(カテゴリ 4)
	取得時期	2006 年	1999 年
	認定機関	TUV	TUV BGIA(ﾄﾞｲﾂ法令労災保険協会)
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・技術ｻﾎﾟｰﾄをする団体。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取りまとめて提出する団体。	
販売	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/	
	価格		
	販売時期	2006 年	
	製品情報	http://www.as-i.jp/prd_sms1.html	
利用ガイド		制御ネットワークに AS-i を使用していれば、非常停止スイッチ等のセーフティ機器を追加するために利用できる。	



セーフティモニタは、AS-i マスタとセーフティスレーブ間の通信を監視し、異常検出時に安全リレー等を作動させることができる。

出典:日本AS-i 協会の資料から引用

図8.5　AS-i セーフティのシステム構成概念図

SIL3関連製品調査票(14)

種別		システムコンポーネント	
製品名		Preventa XPS MC シリーズ	
製品区分		PLC	
特徴	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、Modbusに対応できる。	
	動作条件/動作環境	設定用のソフトウェアはWindows上で稼働する。	
規格	適合規格	SIL3	ISO13849-1(カテゴリ 4)
	取得時期	2005年1月	
	認定機関	TUV	
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/index.html	
販売	販売元	富士電機機器制御 http://www.fujielectric.co.jp/fcs/jpn/index.html	
	価格	171,000～277,000円	
	販売時期	2007年12月	
	製品情報	欄外参照。	
利用ガイド		現在のシステムで複数のリレー装置を使っていれば、省スペース、省配線のために活用できる。	

製品情報のURL:

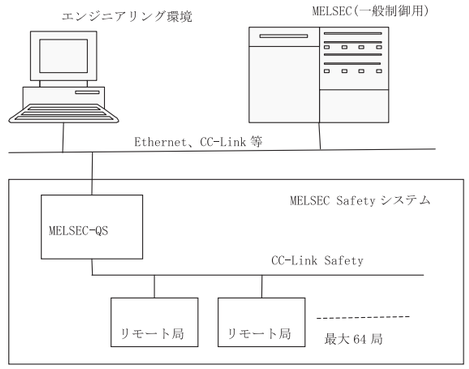
http://www.fujielectric.co.jp/fcs/jpn/f/f_SE_h02-PreventaXPSM_Series.html

SIL3関連製品調査票(15)

種別		システムコンポーネント	
製品名		MELSEC Safety	
製品区分		PLC	
特徴	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。	
	動作条件/動作環境	プログラミングツールは、PC上で稼働する。	
規格	適合規格	SIL3	ISO13849-1(PLe)
	取得時期	2008年3月	同左
	認定機関	TUV	同左
開発元		三菱電機 http://www.mitsubishielectric.co.jp/corporate/tech/index.html	
販売	販売元	三菱電機 欄外参照。	
	価格		
	販売時期	販売中	
	製品情報	http://wwwf2.mitsubishielectric.co.jp/plcq/safety/index_j.htm	
利用ガイド		● リレー回路からのプログラマブル化を実現。 ● リモート局との接続がネットワーク化しているから、省配線、大規模対応を実現できる。	

販売元のURL:

http://www.mitsubishielectric.co.jp/business/industry/equipment/index.html



GX Developer ツールはエンジニアリング環境で稼働する。

図8.6　MELSEC Safetyシステム構成概念図

SIL3関連製品調査票(16)

種別		システムコンポーネント
製品名		GuardPLC システム
製品区分		PLC
特徴	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。
	動作条件/動作環境	
規格	適合規格	SIL3
	取得時期	
	認定機関	
開発元		Rockwell Automation(米国) http://www.automation.rockwell.com/
販売	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/
	価格	
	販売時期	
	製品情報	欄外参照。
利用ガイド		

製品情報:

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

SIL3関連製品調査票(17)

種別		アクチュエータ	
製品名		緊急遮断用アクチュエータ（ＨＡＳ型）	
製品区分		アクチュエータ	
特徴	主要機能	１．高い耐久性 ・動力伝達部は耐久性を最も重視した構造を採用。２００万回を超える社内試験をクリアしている。 ・本体材料にはダクタイル鋳鉄を採用。 ２．安全 ・カートリッジ式のスプリングユニットを採用。スプリングの飛び出しを防止する。 ・擦動部のシリンダ内面はコーティングを施し、始動時の抵抗を軽減し確実に作動します。 ・外部に露出したシャフト上部は２重の防水シールを採用し雨水等の浸入を防ぐ。	
	動作条件/動作環境	●	
規格	適合規格	SIL3	
	取得時期	2009 年 7 月	
	認定機関		
開発元		ＫＩＴＺ http://www.kitz.co.jp/	
販売	販売元	ＫＩＴＺ http://www.kitz.co.jp	
	価格		
	販売時期	販売中	
	製品情報	http://www.kitz.co.jp/product/use_products/has2.html	
利用ガイド		● 石油コンビナート等のプラントにおける緊急遮断弁に使われる。	

SIL3関連製品調査票(18)

種別		RTOS カーネル
製品名		QNX Neutrino RTOS セーフ　カーネル
製品区分		RTOS
特徴	主要機能	・ハイ アベイラビリティ ソリューション ・どのコンポーネント（低レベルドライバも含む）に障害が発生しても、カーネルや他の コンポーネントに影響を与えない ・コンポーネントに障害が発生した場合に、リブートせずに OS がそのコンポーネントをクリーンに終了し、リソースを回復するプロセスモデル ・IPv4、IPv6、IPSec、FTP、HTTP、SSH、Telnet などの主要なネットワーキング技術 ・Photon microGUI – フル機能を装備した組み込みグラフィカルユーザーインターフェイス ・フラッシュ デバイスと回転メディア用の統合ファイル システム ・システムの視認性とデバッ グ サポート ・Eclipse ベースの統合開発環境、フルメモリ保護、システムイベントのトレース ・スケーラビリティ：目的のコンポーネントのみを使用したスケールアップまたはスケールダウン 、ビルトインマルチプロセシング機能、ビルトイン透過分散処理による、耐障害性に優れたクラスタ設計の簡素化 ・ポータビリティ ・POSIX 標準に対する幅広いサポー トにより、アプリケーションのポータビリティを最大限に 高め、Linux、Unix、その他のオープン ソース プログラムからの迅速な移行を実現 ・組み込みシステムに最適なハードウエアプラットフォームの数々に対応。MIPS、PowerPC、SH-4、ARM、StrongArm、XScale、x86 などの一般的なチップセットに対して、ランタイムと BSP のサポートを提供し、システムの迅速な立ち上げを実現 ・ドライバ、アプリケーショ ン、カスタム OS サービスなど 、検証済みのバイナリを製品ライン全体で再利用可能
	動作条件/動作環境	
規格	適合規格	SIL3
	取得時期	2010 年 7 月
	認定機関	TUV
開発元		QNX ソフトウェアシステムズ http://qnx.co.jp/products/intl/neutrino_rtos/
販売	販売元	QNX ソフトウェアシステムズ http://qnx.co.jp/products/intl/neutrino_rtos/
	価格	
	販売時期	販売中
	製品情報	
利用ガイド		医療機器から、インターネットルーター、テレマティクスデバイス、緊急電話センター、プロセス制御アプリケーション、航空管制システムまで、さまざまな基幹システム

SIL3関連製品調査票(19)

種別		ソフトウェアコンポーネント	
製品名		SCIOPTA ARM IEC 61508-P3	
製品区分		RTOS	
特徴	主要機能	- Message-based Architecture and Methodology. - Low memory footprint allows singlechip and SoC applications. - High performance. - All data in a SCIOPTA system are encapsulated in messages. - No shared memory and global data. - SCIOPTA messages have identities. - SCIOPTA messages have ownership. Only the owner of a message can access it. Therefore message data is always protected from concurrent access. - Selective receiving of messages. - Unique and efficient memory management of SCIOPTA messages avoids memory fragmentation. - Easier system design and teamwork by the neat message interface. - System level debugger includes message trace, system inspection and message pool analyzing. - Centralized error handling	
	動作条件/動作環境		
規格	適合規格	SIL3	
	取得時期		
	認定機関	TUV ミュンヘン	
開発元		SCIOPTA(スキオプタ)システム(スイス) http://www.sciopta.com/	
販売	販売元	SCIOPTA(スキオプタ)システム(スイス) http://www.sciopta.com/	
	価格		
	販売時期	販売中	
	製品情報	http://www.sciopta.com/	
利用ガイド		自動車、鉄道、航空、石油精製、科学処理プラント、原子力発電プラント、医療エレクトロニクスなどセーフティクリティカルな分野において数多く利用されている。	

SIL3関連製品調査票(20)

種別		システムコンポーネント	
製品名		セーフティネットコントローラ G9SP	
製品区分		PLC	
特徴	主要機能	・スタンドアロンの安全コントローラ ・G9SPシリーズは安全入出力点数の異なる3種類をご用意 ・標準制御用として4種類の拡張I/Oユニットを 2台まで増設可能 ・イーサネット、シリアル通信で安全システムの モニタリングが可能 ・非接触式ドアスイッチやマットスイッチ等の 多彩な入力機器が接続可能 ・設計、検証、部品化、再利用が可能な プログラミングツール（コンフィグレータ）をご用意	
	動作条件/ 動作環境		
規格	適合規格	SIL3	IS013849-1(Pre)
	取得時期	2010年9月	
	認定機関	TUV	
開発元		オムロン http://www.omron.co.jp/r_d/index.html	
販売	販売元	オムロン http://www.fa.omron.co.jp/index.html	
	価格		
	販売時期	販売中	
	製品情報	http://www.fa.omron.co.jp/	
利用ガイド		小規模から中規模の安全アプリケーションに最適	

SIL3関連製品調査票(21)

種別		ツール	
製品名		MKS INTEGRITY	
製品区分		認証支援	
特徴	主要機能	・ソフトウェア開発の要件、モデル、ソース、テストのすべてに渡ってプロセス、全成果物を最適にコーディネイトし、ソフトウェアエンジニアリングに調和をもたらす総合ＥＣＭソリューション。 ・業界最強のトレーサビリティや変更管理機能により、ISO 26262やAutomotive SPICEへの対応が可能。 ・ソフトウェアエンジニアリングのすべてのフェーズ、すべての成果物を単一アーキテクチャ、単一リポジトリで管理する。	
	動作条件/ 動作環境		
規格	適合規格		
	取得時期		
	認定機関		
開発元		MKS INTEGRITY　株式会社 http://www.mks-integrity.jp	
販売	販売元	MKS INTEGRITY　株式会社 http://www.mks-integrity.jp	
	価格		
	販売時期	販売中	
	製品情報	http://www.mks-integrity.jp/product/index.html	
利用ガイド		トレーサビリティ管理に最適	

SIL3関連製品調査票(22)

種別		ツール	
製品名		C++test7.3.2	
製品区分		認証支援	
特徴	主要機能	・C/C++ プログラムの単体テスト、静的解析、フロー解析、実行時メモリエラー検出の自動化をサポートし、高品質なソフトウェアの開発を実現するための総合的なテストツールです。 ・上記の４つの検証機能は、堅牢で高品質なC/C++ アプリケーションの開発とテスト工数の大幅削減を可能にします。これらの４つの検証機能は、クロスコンパイル後にシミュレータやターゲット機でテストを実行するような組み込みソフトウェアの検証にも使用できます。 ・機能安全規格に含まれるソフトウェアに関する要件では、コーディング標準に対する適合性や単体テストの実施、テストのカバレッジ収集などが推奨されており、規格に適合したソフトウェア開発環境の構築を支援する。	
	動作条件/動作環境	Windows、Linux、Solaris、AIX	
規格	適合規格	IEC 61508	
	取得時期	2010 年 11 月	
	認定機関	TUV SUD	
開発元		PARASOFT CORPORATION http://www.parasoft.com	
販売	販売元	テクマトリックス株式会社 http://www.techmatrix.co.jp	
	価格		
	販売時期	販売中	
	製品情報	http://www.techmatrix.co.jp/quality/ctest/	
利用ガイド		ソフトウェアの品質向上と効率的な開発の実現をサポート	

第3章
機能安全用語調査

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。 ALE＝F×I＜F：年間に損失が発生する予想頻度，I：1回あたりの予想損失額＞	
	ASIL	Automotive Safety Integrity Level	one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level	ISO 26262-1.7
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: Britsh 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	dedicated measures	dedicated measures	measures to ensure the failure rate claimed in the evaluation of the probability of violation of safety goals	ISO 26262-1.20
	degradation	degradation	strategy for providing safety by design after the occurrence of failures	ISO 26262-1.22
	detected fault	detected fault	fault whose presence is detected by a safety mechanism within a prescribed time	ISO 26262-1.23

見出	用　語	英文（略号）	解　説	出 典
	DISC PD3000方式	Delivering Information Solution to Customer（DISC）PD3000 method	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手法。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 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。 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対照的な言語である。	
	dual point failure	dual point failure	failure, resulting from the combination of two independent faults, that leads directly to the violation of a safety goal	ISO 26262-1.29
	dual point fault	dual point fault	individual fault that, in combination with another independent fault, leads to a dual point failure	ISO 26262-1.30
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。	
	element safety function	element safety function	that part of a safety function (see 3.5.1) which is implemented by an element	IEC 61508-4 Ed2 3.5.3
	emergency operation	emergency operation	functionality to transition to a safe-state as defined in the fail-safe concept	ISO 26262-1.34
	emergency operation interval	emergency operation interval	time-span between the occurrence of a fault and transition to a safe state as defined in the fail-safe concept, in which at least the functionality specified as an emergency operation is supported	ISO 26262-1.35
	environment	environment	all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase	IEC 61508-4 Ed2 3.2.2
	ETA	Event Tree Analysis	イベントツリー解析 / 事象の木解析のことで、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

見出	用　語	英文（略号）	解　説	出 典
	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（即ち機能安全に係る当該リスク）の軽減が行わなければならない。 備考2 EUCリスクの決定の主な目的は、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及点を決定することにある。 （備考欄のインデントを修正する）	JIS C 0508-4:1999 3.2.4
	EUC制御系	EUC Control System	″ﾌﾟﾛｾｽ及び／又はｵﾍﾟ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
	exposure	exposure	state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis	ISO 26262-1.37
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だすために、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。	
	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ー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	harmful event	harmful event	occurrence in which a hazardous situation or hazardous event results in harm	IEC 61508-4 Ed2 3.1.5
	hazardous event	hazardous event	combination of a hazard and an operational situation	ISO 26262-1.59

見出	用　語	英文（略号）	解　説	出 典
	HAZOP	Hazard and Operability Study	リスクシナリオ分析手法の一つで、化学ﾌﾟ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。特に設計仕様（例えば、温度、圧力、PH、撹拌、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ｽﾞﾚの発生個所及びそこで発生するﾊｻﾞｰﾄﾞ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。目標値からのｽﾞﾚを想定するために、「ｶﾞｲﾄﾞﾜｰﾄﾞ」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 Electro technical 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
	inde pendence	inde pendence	absence of dependent failure between two or more elements that could lead to the violation of a safety requirement; or organizational separation of the parties performing an action	ISO 26262-1.61
	independent failures	independent failures	failures whose probability of simultaneous or successive occurrence can be expressed as the simple product of their unconditional probabilities	ISO 26262-1.62
	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
L	latent fault	latent fault	multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval	ISO 26262-1.71

見出	用　語	英文（略号）	解　説	出 典
M	MISRA	The Motor Industry Software Reliability Association	MISRAは欧州の自動車業界団体の略称。自動車用の安全なシステムの開発方法の普及を目指す、自動車メーカ、部品メーカ、研究者からなる協会（http://www.misra.org.uk/）。自動車用の安全なシステムの開発方法の普及を目指す、自動車メーカ、部品メーカ、研究者からなる協会（http://www.misra.org.uk/）。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」や機能安全に対処する実務ガイドライン「MISRA-SA」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 IDENTIFI CATION. TECHNIQUES"、HSL/2005/58 6.2.5
	MTTR	Mean Time To Repair	平均修復時間。修復時間の期待値。 備考　JIS Z 8115では，英文名として他に，Mean Time To Restoration, Mean Time To Recoveryがある。"	JIS Z 8115
	multiple point failure	multiple point failure	failure, resulting from the combination of several independent faults, which leads directly to the violation of a safety goal	ISO 26262-1.76
	multiple point fault	multiple point fault	individual fault that, in combination with other independent faults, leads to a multiple point failure	ISO 26262-1.77
	multiple point fault detection interval	multiple point fault detection interval	time span to detect multiple point fault (1.77) before it may contribute to a multiple point failure	ISO 26262-1.78
O	overall safety function	overall safety function	means of achieving or maintaining a safe state for the EUC, in respect of a specific hazardous event	IEC 61508-4 Ed2 3.5.2
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	これまでのﾊｻﾞｰﾄﾞまたは故障の経験、知識によって、危害やﾊｻﾞｰﾄﾞを招く恐れのある事象を特定し、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。開発ﾌﾟﾛｼﾞ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
	process safety time	process safety time	period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring	IEC 61508-4 Ed2 3.6.20

見出	用　語	英文（略号）	解　説	出 典
	proven in use	proven in use	demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level	IEC 61508-4 Ed2 3.8.18
R	residual fault	residual fault	portion of a fault that by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by safety mechanisms	ISO 26262-1.94
	residual risk	residual risk	risk remaining after the deployment of safety measures	ISO 26262-1.95
	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	safety architecture	safety architecture	set of elements and their interaction to fulfill the safety requirements, including redundancy and independence concepts	ISO 26262-1.102
	safety goal	safety goal	top-level safety requirement as a result of the hazard analysis and risk assessment	ISO 26262-1.105
	safety measure	safety measure	activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures,, or mitigate their harmful effects	ISO 26262-1.106
	safety mechanism	safety mechanism	measure implemented by a E/E functions or element, or in other technologies, to detect or control failures in order to achieve a safe state of the item, or maintain a safe state of the item, or both	ISO 26262-1.107
	safety plan	safety plan	plan to control and guide the safety activities of a project including dates, milestones, tasks, deliverables, responsibilities and resources	ISO 26262-1.108
	safety-related element	safety-related element	element which has the potential to contribute to the violation of a safety goal	ISO 26262-1.109
	safety-related special characteristic	safety-related special characteristic	product or production process characteristic for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of functional safety	ISO 26262-1.110
	safety validation	safety validation	assurance, based on examination and tests, that the safety goals are sufficient and have been achieved	ISO 26262-1.111
	SIL	Safety Integrity Level	安全度水準に同じ。	JIS C 0508-4:1999 3.5.6
	single point failure	single point failure	failure that results from a single point fault and leads directly to the violation of a safety goal	ISO 26262-1.116
	single point fault	single point fault	fault in an element that is not covered by a safety mechanism and that leads directly to the violation of a safety goal	ISO 26262-1.117
	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

見出	用　語	英文（略号）	解　説	出 典
	systematic capability	systematic capability	measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element	IEC 61508-4 Ed2 3.5.9
T	target risk	target risk	risk that is intended to be reached for a specific hazard taking into account the EUC risk together with the E/E/PE safety-related systems and the other risk reduction measures	IEC 61508-4 Ed2 3.1.10
	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発された。	
	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。形がV字型のためこの名がある。	
W	What-if	What-if	非体系なブレー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

見出	用　語	英文（略号）	解　説	出 典
	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、λ = λS + λD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。 (λS + λDD) / (λS + λD) < λS :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）が含まれなければならない。 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。 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

見出	用　語	英文（略号）	解　説	出 典
	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
	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、即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ﾌﾞｲﾘ事故の原因調査 ・ 分析の結果をきっかけとして生まれた。その時国際原子力機関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「ﾁｪﾙﾉﾌﾞ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。本質的安全設計方策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策。 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	SRSへの作動要求頻度の観点から区分するSRSの使用法。低頻度作動要求ﾓｰﾄﾞか、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又は複数の人。	*) TR B 0008、3.21

見出	用　語	英文（略号）	解　説	出 典
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。 — 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。 — 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、かつそれらを用いず、リスク軽減又は緩和する手段。例えば、排出装置、防火壁、堤防等。	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 ・ ﾚｼﾞｽﾀﾝｽ）、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。	
	感度分析	Sensitivity analysis	どのリスクがﾌﾟﾛｼﾞ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ﾍﾞｰｽﾗｲﾝ値（基準値）に固定した状態で、ﾌﾟﾛｼﾞ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）を危険な方向即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

見出	用　語	英文（略号）	解　説	出 典
	危険側故障率	Frequency of a Dangerous Failure per Hour（PFH）	時間当たりの危険側故障の率をいう。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等により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、電気的危険源）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潰しの危険源,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、電気的危険源、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合せ。個々には些細とみられる危険源であっても、これらが互いに組合さ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。 本質安全と対比される用語。	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、ときに人も含まれる。	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	

見出	用　語	英文（略号）	解　説	出 典
	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	現今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
	組込みシステム	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ﾋﾟ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やｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄｳｪｱ等）とﾊｰﾄﾞ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，代数学等の数学を基礎としたｼｽﾃﾑの仕様記述手法，検証手法等の総称。要求，仕様，設計等を自然言語ではなく、形式的言語で記述することにより、曖昧さを排除し、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易く、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等の記法の他、truth tables等の手法がある。	
	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。SIL 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。システマティック故障に同じ。	JIS C 0508-4:1999 3.6.6
こ	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。	
	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

見出	用　語	英文（略号）	解　説	出 典
	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、プルーフテスト頻度の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
	コートニィ理論	Courtney Theory	1992年英国のリチャード ・ コートニィ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なること、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（システマティック故障）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エ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。	
	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、この場合特に原子炉の固有の安全性と呼んでいる。	
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

見出	用　語	英文（略号）	解　説	出 典
	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。 — 設計者が保護方策を講じた後の残留リスク — 全ての保護方策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（DC）	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。 備考　この定義は、次の式によっても表現してよい。DC= Σ λ DD/ Σ λ total　ここにDCは自己診断率、Σ λ totalは危険側故障率、およびλDDは危険側故障率のうち検出可能な部分である。	JIS C 0508-4:1999　3.8.6
	システマティック安全度	Systematic safety integrity	決定論的原因安全度参照。	
	システマティック故障	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。	
	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て使う。	Think IT
	シミュレーション法	Simulation method	モデルを作り、ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞ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

見出	用　語	英文（略号）	解　説	出 典
	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時に、ある状態から別の状態に移ることを図式化した図。時間の経過や状況の変化に基づいて、その時の動作を記述する。状態を円で、状態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ﾃﾞ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。	
	初期故障期間 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
	信頼性	reliability	ｱｲﾃﾑが与えられた条件下で、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
す	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
せ	制御機器	Control device	制御回路の中にあっ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

見出	用　語	英文（略号）	解　説	出 典
	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、ｿﾘﾉｲﾄﾞｽｲｯﾁ、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	Control gear	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合せ。 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そ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	ﾌﾟ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、ｺﾝﾄﾛｰﾙｺﾝﾋﾟｭｰﾀ、制御ｺﾝﾋﾟｭｰﾀ、ﾌﾟﾛｾｽｺﾝﾋﾟｭｰﾀ等とも呼ばれる。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 ・ ﾌﾟﾛｸﾞﾗﾑを実行することなく、ｿｰｽｺｰﾄﾞの品質を測定／評価し、ｿｰｽｺｰﾄﾞに内在する問題を改善するためのﾂｰﾙ。ﾌﾟﾛｸﾞﾗﾑに対して、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ﾊﾟ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等）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。	

見出	用　語	英文（略号）	解　説	出 典
	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）」など、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
そ	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る。 備考2 ソフトウェアは、保全できないので部分改修される。	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、安全機能の安全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 3.5.8 参照。
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。	

見出	用　語	英文（略号）	解　説	出 典
	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下で実施。 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どうかを決定するために、開発ﾌﾟﾛｾｽの最終段階で、ｼｽﾃﾑ及びその構成部品を評価、実証するﾌﾟﾛｾｽ。	JIS Z 8115 JIS C 0508-4 3.8.2
ち	チャネル	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チャネル構成とは、同一の機能を独立して実行する2チャ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）を表現することもできる。	JIS C 0508-4:1999 3.3.8
つ	ツー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
て	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。ﾘｽｸ発生時のﾌﾟﾛｼﾞ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、品質等のﾌﾟﾛｼﾞｪｸﾄの制約条件に対するﾘｽｸ許容度等の要因を査定する。	
	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。 －各々の部品のフォールトモードが明確に定義される。 －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。信頼性改善のため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、定格値を下回る値で使用すること。部品故障はｽﾄﾚｽの累積によって引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）。このｽﾄﾚｽ軽減がﾃﾞｨﾚｰﾃｨﾝｸﾞと呼ばれるもので、例えば、電子部品の主要なｽﾄﾚｽは、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ﾃﾞｨﾍﾟﾝﾀﾞﾋﾞﾘﾃｨ（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。	JIS Z 8115 JIS C 0508-4:1999 3.8.1

見出	用　語	英文（略号）	解　説	出 典
	デシジョン ・ 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って）確認する施設が含まれる。	JIS C 0508-4:1999 3.8.15
	デルファイ法	Delphi method	多くの専門家が夫々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、という作業を繰返し行うことで、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手法。米国の研究機関ﾗﾝﾄﾞｺｰﾎﾟﾚｰｼｮﾝが開発した。	
	電磁耐性	Electro magnetic 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賀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を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	SRSの安全度のうち、危険側機能失敗に導くﾗﾝﾀﾞﾑﾊｰﾄﾞｳｪｱ故障に係る部分。 備考 ： これは、SRSの安全度を損なう危険側故障に関連した用語。ここで関係する2個のﾊﾟﾗﾒｰﾀは、SRS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。前者の失敗ﾊﾟﾗﾒｰﾀは、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、後者のﾊﾟﾗﾒｰﾀはSRS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ﾊﾞｰﾄﾞ ・ 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。	

見出	用　語	英文（略号）	解　説	出 典
	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。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も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。 - 人間の単一動作によって停止指令を出す。 詳細はJIS B 9703参照。	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	安全側の故障ﾓｰﾄﾞになる確率が危険側の故障ﾓｰﾄﾞになる確率よりも著しく高い特性。	
	人	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
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

見出	用　語	英文（略号）	解　説	出 典
	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、遮断及びｴﾈﾙｷﾞ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種で、「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。ﾌﾟﾛｸﾞ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。ﾌﾟﾛｸﾞﾗﾑのｿｰｽｺｰﾄﾞから、線形的に独立した経路の数を直接数える。	
	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
	プルーフテスト	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”又は実際上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 ﾌﾟﾙｰﾌﾃｽﾄの効果は、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。ﾌﾟﾙｰﾌﾃｽﾄが十分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。 ﾌﾟﾙｰﾌﾃｽﾄを実施する時間間隔をﾌﾟﾙｰﾌﾃｽﾄ間隔という。	JIS C 0508-4:1999 3.8.5
	プルーブン・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、危険側システマ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。	
	ブレーンストーミング法	Brain storming	複数メンバーが自由にｱｲﾃﾞｱを出し合い、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ﾃﾞｱを生み出そうという集団思考法 ・ 発想法。 1940年前後に米国の広告業界で創案されたが、その狙いは“つまらないｱｲﾃﾞｱでも、他の出席者には別の素晴らしいアイデアを閃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ﾃﾞｱを出すと、彼はほとんど自動的に別のｱｲﾃﾞｱに対する創造力をかき立てる。それと同時に彼のｱｲﾃﾞ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。	

見出	用　語	英文（略号）	解　説	出 典
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。MTFFdを求めるには、安全関連部をI ： 入力、L ：論理、O ： 出力 に分けて夫々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）	
ほ	防御的プログラミング	Defensive programming	不正入力があっても、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注意深く慎重を期したプログラミング。	
	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。次によって実行される。 ― 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なら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	固有安全ともいい、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。機能安全と対比される。	
	本質的安全設計方策	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策。 注記　本質的安全設計方策には、例えば次のような方策がある。 ― 幾何学的要因及び物理的側面を考慮した方策 ― 機械設計上の一般的技術知識を考慮した方策 ― 適切な技術選択による方策 ― 構成品間のポジティブな機械的作用原理を適用した方策 ― 機械の安定性に関する方策 ― 機械の保全性に関する方策 ― 人間工学原則を考慮した方策 ― 電気的危険源防止方策 ― 空圧／液圧設備の危険源防止方策 ― 制御システムへの本質的安全設計方策の適用 ― 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策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

見出	用　語	英文（略号）	解　説	出 典
	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、その確率ﾓﾃﾞﾙをﾏﾙｺﾌﾓﾃﾞﾙという。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系に、状態遷移確率が時間に依存するﾏﾙｺﾌﾓﾃﾞ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。	JIS B 9704-2、3.6
	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、ﾊｰﾄﾞｳｪｱの多様な劣化ﾒｶﾆｽﾞﾑから生じる故障。 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ｽﾞﾑが存在し、製造上の許容誤差がそれらのﾒｶﾆｽﾞﾑによって運転中の部品故障を異なる時刻に引起す。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. ﾗﾝﾀﾞﾑﾊｰﾄﾞｳｪｱ故障とｼｽﾃﾏﾃｨｯｸ故障を区別する主な性質は、ﾗﾝﾀﾞﾑﾊｰﾄﾞ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、ｼｽﾃﾏﾃｨｯｸ故障（による機能失敗）が、正確には予測できない点にある。即ち、ﾗﾝﾀﾞﾑﾊｰﾄﾞ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、ｼｽﾃﾏﾃｨｯｸ故障によるものは、故障へと導く事象が容易には予測できないので、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
	リスク解析	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 12100-1:2003）

見出	用　語	英文（略号）	解　説	出 典
	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（a，b，c，d，eの5段階に振り分けられる）を2分法の図で表現したもの。	
	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
	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ｸｽのこと。そして、それぞれのﾘｽｸを影響度と発生確率によってﾏｯﾋﾟﾝｸﾞしていき、高ﾘｽｸ（例:赤色）、中ﾘｽｸ（例:黄色）、低ﾘｽｸ（例:緑色）に色分けしていくことで、ﾌﾟﾛｼﾞｪｸﾄのﾘｽｸの状況を一瞥できるﾏﾄﾘｸｽ。	
	リスクマネジメント	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に一連の情報をシステム的に利用する。	TR Q 0008:20003
	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、対応が必要かを判断するための基準。	
	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

見出	用　語	英文（略号）	解　説	出 典
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（アクチェータ等）を除いた部分。	JIS C 0508-4、3.4.5
よ	予期しない起動	Unexpected start-up、Unintened 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1　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2「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。
出典欄の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。
安全設計の基本知識は平成20年度版に記載しており、いろいろな事例や最新動向については平成21年度版と本書22年度版を参照いただきたいと思います。
機能安全は、まだ発展途上です。そのため、製品調査も用語集もまだまだやり残しております。
来年度以降は、製品調査と用語編集を継続活動とし、新たな課題として、昨年末のET2010セミナーで頂いたご要望、ご指摘事項を考慮して、ISO 26262やSPICE、安全設計のより実践的手法などを調査・研究していきたいと思います。
また、本報告書をご覧になり、我々の活動への参加、ご提言などを頂けたら、たいへんありがたく存じます。

平成２３年３月

製品安全ワーキンググループ
主査　金田光範

＊＊＊　第2部の執筆者一覧　＊＊＊

ＪＡＳＡ　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 ）	ｱｯﾌﾟｳｨﾝﾄﾞﾃｸﾉﾛｼﾞｰ ・ ｲﾝｺｰﾎﾟﾚｲﾃｯﾄﾞ
竹岡 尚三	（ 委員 ）	株式会社アックス
田渕 一成	（ 委員 ）	ﾋﾞｼﾞﾈｽｷｭｰﾌﾞ・ｱﾝﾄﾞ・ﾊﾟｰﾄﾅｰｽﾞ株式会社
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
竹市 正彦	（アドバイザー）	日本TUV
門田 浩	（アドバイザー）	JASA

添付資料

ET2010技術本部セミナーで使用されたプレゼン資料

組込みシステムの機能安全

１．　ＪＡＳＡ委員会活動紹介
２．　組込みシステムにおける安全設計
３．　機能安全設計の基本
４．　機能安全の将来動向と教育体系

組込みシステムの機能安全

安全性向上委員会　製品安全WG

金田　光範　　東芝システムテクノロジー株式会社
水口　大知　　(独) 産業技術総合研究所
兼本　茂　　会津大学　教授

司会　入月　康晴　　(地独)東京都立産業技術研究センター

社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

1

セミナー内容

Ⅰ. JASA委員会活動紹介 ⇨
入月康晴
Ⅱ. 組込みシステムにおける安全設計
金田光範
Ⅲ. 機能安全設計の基本
水口大知
Ⅳ. 機能安全の将来動向と教育体系
兼本　茂

2

Ⅰ. JASA委員会活動紹介

1. 組込み系の動向
2. JASAの活動経過
3. 機能安全セミナー開催
4. 機能安全用語集
5. 機能安全製品一覧

3

組込み系を取り巻く主な動き

1998/11～2000/5　IEC 61508発行(JIS C 0508)　「機能安全」が規格として登場
2003/10　経産省、「組込みソフトウェア開発力強化推進委員会準備会」を立上げ
2004/10　IPAがSEC(Software Engineering Center)設立
2006/ 3　JST畑村委員会、失敗知識データベースをWeb掲載
2006/ 4　経産省、機能安全を基盤技術に指定　　(株)日本機能安全　発足
2006/ 6　経産省、「情報システムの信頼性向上に関するガイドライン」を公表
2006/11　SEC、「組込みシステムの安全性向上の勧め」小冊子発行
2009/ 3　経産省、「情報システムの信頼性向上に関するガイドライン」第2版公表
2010/4　IEC 61508 第2版発行
2011/6　ISO 26262 IS 発行予定

4

JASAの活動

2006/6　機能安全委員会(現 安全性向上委員会)発足
2007/4　機能安全に関する調査研究の3年計画スタート
2008/3　「組込みシステムにおける機能安全に関する調査研究」発行
(報告書:情報セキュリティと機能安全)
2009/3　「組込みシステムにおける機能安全に関する調査研究」発行
(報告書:安全設計入門)
2010/3　「機能安全に関する調査研究」発行
(報告書:事例調査、安全関連製品集作成、安全用語集作成)
2010/7　「組込み系技術者のための安全設計入門」発刊　(業界初)

5

安全性向上委員会　製品安全WG

漆原 憲博	(委員長)	株式会社ジェーエフピー　社長
金田 光範	(WG主査)	東芝システムテクノロジー株式会社　技術顧問
大塚 悦生	(委員)	東芝システムテクノロジー株式会社　主幹
入月 康晴	(委員)	(地独) 東京都立産業技術研究センター　主任研究員
済賀 宣昭	(委員)	東海ソフト株式会社　顧問
那須 誠	(委員)	株式会社ジェーエフピー　役員
藤原隆次	(委員)	ビジネスキューブ・アンド・パートナーズ(株) シニアディレクタ
中村 憲一	(委員)	アップウィンドテクノロジー・インコーポレイテッド　社長
竹岡 尚三	(委員)	(株)アックス　会長
六反田 喬	(委員)	ガイオ・テクノロジー株式会社　顧問
中村 洋	(委員)	(株)レンタコーチ　社長　他10数名
竹市 正彦	(アドバイザー)	テュフズードジャパン株式会社　機能安全部エンジニア
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) 産業技術総合研究所　計測標準研究部門
門田 浩	(アドバイザー)	社団法人組込みシステム技術協会 (JASA) 事務理事
前澤 敏昭	(事務局)	社団法人組込みシステム技術協会(JASA) 課長

6

機能安全セミナーの開催

開催日		テーマ	講師
2008	7/30	課題提起：安全なソフトウェアとはなにか	日本機能安全　吉岡律夫 氏 三菱電機　神余浩夫 氏
2009	7/17	規格紹介：製品安全の確保と認証取得	IDEC　前田育男 氏 TÜV SÜD Japan　竹市正彦 氏
	9/18	事例紹介：産業機械部品分野、自動車分野	ジェイテクト　宮脇信芳 氏 日産　山下修平 氏
	10/16	事例紹介：原子力分野、ソフトウェア分野	テクノバ　藤田祐志 氏 ビジネスキューブ&パートナーズ　藤原隆次 氏
	11/27	事例紹介：鉄道分野、制御機器分野	日本大学　中村　英夫 氏 IDEC　伊佐　泰夫 氏
2010	2/24	事例紹介：機械・電子部品、宇宙分野のソフトウェア	オムロン　河野秀明氏 JAXA　片平真史氏
	4/27	規格紹介：IEC61508改訂版とISO26262の最新動向	東京海洋大学　佐藤吉信氏 TÜV SÜD Japan　竹市正彦氏
	6/21	事例紹介：医療電気機器分野、ドイツ産業分野	都立産業技術研究センター　岡野　宏氏 シーメンス　雨宮祐介氏
	8/23	技術紹介：セーフウエアと形式手法の実践的試み	日本機能安全　吉岡律夫 氏 名古屋市工業研究所　小川 清 氏

7

機能安全に関する用語

用語集サンプル

FrontPage/単語帳/機能安全用語集

http://jasa.or.jp/sa/index.php?FrontPage%2F%C3%B1%B8%EC%C4%A2%2F%B5%A1%C7%BD%B0%C2%C1%B4%CD%D1%B8%EC%BD%B8

[トップ] [編集 | 凍結 | 差分 | バックアップ | 添付 | リロード] [新規 | 一覧 | 単語検索 | 最終更新 | ヘルプ]

最新の20件
2010-04-28 ・MTTR
2010-04-27 ・単語帳/セキュリティ用語集
2010-04-26 ・DISC PD3000方式 ・自己診断率 ・リスクグラフ ・MISRA
2010-04-12 ・FrontPage ・FrontPage/単語帳/機能安全用語集
2010-04-10 ・危険側故障率 ・RecentDeleted
2010-04-04 ・What-if ・Vモデル ・TOE ・TBQ ・SRP/CS ・PHA ・PFD

FrontPage/単語帳/機能安全用語集

機能安全用語集

本用語集は，JASA安全性向上委員会・製品安全ワーキンググループの活動成果の一環として出版された，向殿政男監修の機能安全に関する入門書「組込み系技術者のための安全設計入門」(電波新聞社刊)に出てきた用語をベースにまとめたものです。この活動の中で，用語の統一が入門書にとって，共通理解と情報交換等のために極めて重要であるとの認識が生まれ，本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としてまとめました。

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きました。これに加えて，JIS規格の ② 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」，③JIS Z 8115:2000「ディペンダビリティ(信頼性)用語」，④JIS 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，その他を参照しています。なお，定義の厳密性の点からJIS規格の定義を最優先とし，JIS規格の定義も，規格によって異なるところもあるため，採用の優先順位を上記JIS規格②→③→①/④の順としました。

URL;　http://jasa.or.jp/sa/yougosyu.html

8

安全関連製品の現状

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
ジェイテクト (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ィーユニットG9SX	PLC
TRICONEX社製TRICON/ (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 SafetyONE	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
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
東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／シーディ・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

次ページで一部分紹介

9

安全関連製品事例の紹介（一部抜粋）

PLC

安全計装システム　システムコンポーネント　SIL 3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 年以上の高稼動率の実現
●オンラインメンテナンスとして故障発生時、稼動中の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範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（SIL 3）　http://www.shinkawa.co.jp/triconex/
《販売元》
山武　http://jp.yamatake.com/

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　SIL 3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）　http://www.hima.com/
HIMA JAPAN　http://www.himajapan.com/
《販売元》
日立ハイテクトレーディング　http://www.hitachi-hitec-trading.com/

出典:「組込み系技術者のための安全設計入門」P161

10

参考資料のご紹介

推薦者:向殿政男　(明治大 教授)

時代は製品の安全性確保を強く要請している。

本書は、安全の概念と安全設計の基礎をしっかりと説明したうえで、. . .

これからの安全技術者、組込み技術者の常識となる安全設計の基本を紹介している先進的な本である。
（抜粋）

電波新聞社　発行

11

セミナー各章の要旨

Ⅱ. 組込みシステムにおける安全設計

現代は、あらゆる機器にマイコンが組み込まれる様になってきた。それとともに、ソフトウェアが安全性を担うケースも増えており、電子機器に関する安全規格も普及しつつある。しかし、ソフトウェアで製品の安全を確保するためには、まず安全設計の基礎となる事項をしっかり理解する必要がある。機能安全について理解を深めるためにも、安全とは何か、製品開発に臨むにあたって基本的な事項について述べる。

12

セミナー各章の要旨

Ⅲ. 機能安全設計の基本

昨今、電子制御システムの機能安全に対する関心はますます高まっている。こうした状況を受けて、本講演では、機能安全の基本的な考え方を、IEC 61508に基づいて解説する。とくに、安全関連システムにおける安全度水準(SIL)とその達成方法について、ハードウェア安全度およびシステマティック安全度の側面から説明する。最近発行されたIEC 61508第2版における要求事項の修正点についても述べる。

13

セミナーⅣ章の要旨

Ⅳ. 機能安全の将来動向と教育体系

組み込みシステムの複雑化が進む中で、停止安全という考え方に頼らない高度な安全管理が必要なシステムが今後ますます増えてゆくことが想定される。そのためには、機能安全の本質を理解した上で、規格に準拠した設計を行うことが大切になる。このような考え方から、大学での機能安全に関する講義を最近立ち上げたが、その概要を紹介する。また、併せて、欧米での技術調査を行った結果を紹介し、今後の動向を考察する。

14

セミナー内容

Ⅰ. JASA委員会活動紹介
入月康晴
Ⅱ. 組込みシステムにおける安全設計 ⇨
金田光範
Ⅲ. 機能安全設計の基本
水口大知
Ⅳ. 機能安全の将来動向と教育体系
兼本　茂

15

組込みシステムの機能安全

Ⅱ. 組込みシステムにおける安全設計
～組込みにおける安全とは～

安全性向上委員会　製品安全WG

主査　　金田光範
東芝システムテクノロジー（株）技術顧問

組込みシステム技術協会

1

Ⅱ. 組込みシステムにおける安全設計

1. 組込みシステムの状況
2. 安全に対する関心の高まり
3. 機能安全規格の概要
4. 安全に関する用語と概念の整理
5. ソフトウェアの安全設計

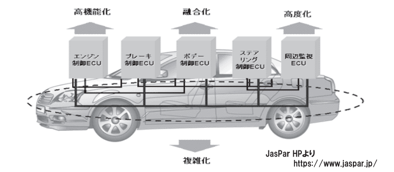
金田　光範

2

組込みシステム開発事例（1/2）

自動車のソフト開発

近年、ソフトウェアで制御するモジュールが急増。

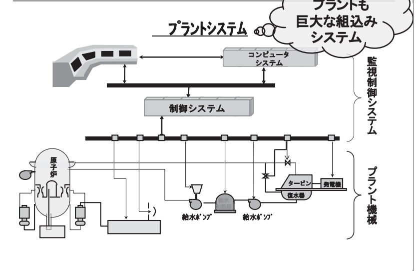


JasPar HPより
https://www.jaspar.jp/

3

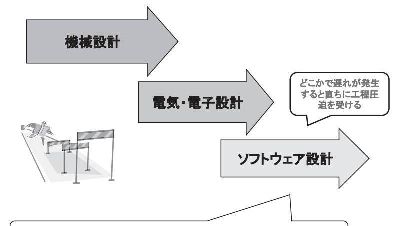
組込みシステム開発事例　(2/2)

プラントも巨大な組込みシステム



4

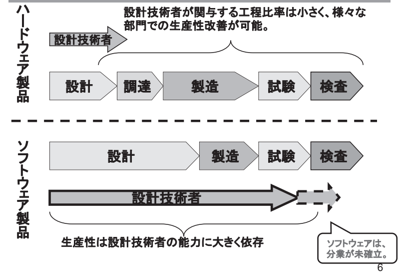
組込み系の課題（1/2）



ソフトウェアは工程の最後尾

5

組込み系の課題（2/2）



6

組込み系の課題（まとめ）

組込み系の開発プロセスには、多くの課題が存在している。特に工程に余裕がない。
もし、
安全規格認証を取ろうとすると、これまでの課題が表面化して、大きな混乱を伴う可能性がある。

しかし、
安全への関心の高まりは、組込み系のプロセス改善のチャンスでもある。

7

Ⅱ. 組込みシステムにおける安全設計

1. 組込みシステムの状況
2. 安全に対する関心の高まり
3. 機能安全規格の概要
4. 安全に関する用語と概念の整理
5. ソフトウェアの安全設計

8

車の電子化リスク

出典元:朝日新聞3面　2010年3月5日

9

過去の大きな事故事例

①スリーマイル原発事故　(1979/3/28)　(大きな教訓となった事故)
死者0、一時避難10万人
②ボパール化学工場事故　(1984/12/3)　(世界最大の化学工場事故)
死者15～25千人、被害15～60万人
③日航ジャンボ機墜落　(1985/8/12)　(世界最大の航空機事故)
死者520人、負傷4人
④チェルノブイリ原発事故　(1986/4/26)　(世界最大の原発事故)
死者31人+α 避難13万5千人
⑤東海村JCO臨界事故　(1999/9/30)　(日本初の死亡&避難事故)
死者2、避難350人、屋内待機10Km以内
⑥JR福知山線脱線事故　(2005/4/25)　(JR史上最悪)
死者107人、負傷者555人
⑦その他　スペースシャトル爆破事故、もんじゅナトリウム漏洩　等々

10

ソフトウェアが関係した事故状況

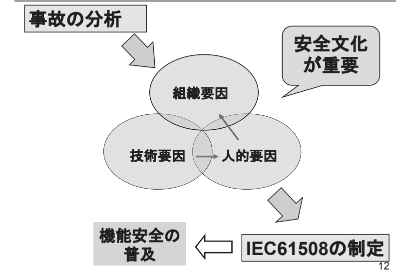
ソフトウェアが直接関与した事故も大きな話題。

例えば、
- アリアンロケット打ち上げ失敗　(1996/ 6/ 4)
- ANA　国内線予約システム障害　(2007/ 5/27)
- 自動改札機のトラブル　(2007/10/12)
- 東証のシステム障害再々発　(2008/ 7/22)
- 携帯電話、デジタルTV、自動車リコール　等々

背景　:
・大規模な計算機システムが社会インフラに組込まれるようになった。
・身近な製品にもマイコンが多用される時代になった。

11

重大事故に潜む3つの要因



12

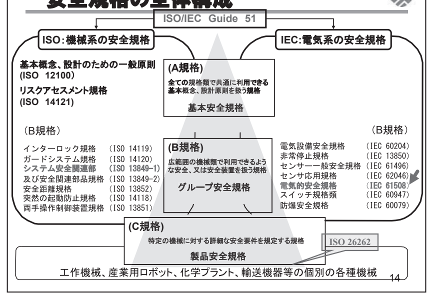
Ⅱ. 組込みシステムにおける安全設計

1. 組込みシステムの状況
2. 安全に対する関心の高まり
3. 機能安全規格の概要
4. 安全に関する用語と概念の整理
5. ソフトウェアの安全設計

·安全規格の全体構成
·IEC 61508 の概要
·機能安全とは、SIL、SRSについて。
·安全ライフサイクル、ベストプラスティス
·ISO 26262　の概要
·規格認証

13

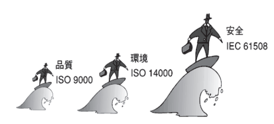
安全規格の全体構成



14

IEC 61508 について　(1／4)

1980年代になってから多くの産業事故の発生とコンピュータ技術の普及に密接に関係して、安全の専門家によって考え方が検討され、国際電気標準会議(IEC)によって制定された安全規格です。
機能安全は、ISO 9000、ISO 14000　に続く第三のコンプライアンスです。



注:(株)日本機能安全HPから抜粋引用

15

IEC 61508 について　(2／4)

●IEC 61508 (JIS C0508)　1998～2000
Functional safety of electrical/electronic/programmable electronic safety-related systems
電気・電子・プログラマブル電子安全関連系の機能安全

●IEC 61508 (JIS C0508)　*2010 年4月　第2版発行*

安全関連系のハードウェア/ソフトウェアの設計指針であり、業務遂行に関するマネジメントの規格でもある。
規格は350ページに及び、リスク評価・安全度水準、全安全ライフサイクル・機能安全評価・ハードウェア/ソフトウェア技法の導入など、これまでに無い規格構造を有している。　注：(株)日本機能安全HPから抜粋引用

16

IEC 61508 について　(3／4)

IEC61508(JIS C 0508)の構成

		制定年	頁数
第1部	一般要求事項 General Requirements	1998	115 (52)
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 Requirements for electrical/electronic/programmable electronic safety-related systems	2000	143 (52)
第3部	ソフトウェア要求事項 Software requirements	1998	93 (44)
第4部	用語の定義及び略語 Definitions and abbreviations	1998	53 (28)
第5部	安全度水準決定方法の事例 Examples of methods for the determination of safety integrity levels	1998	57 (28)
第6部	第2部及び第3部の適用指針 Guidelines on the application of IEC 61508-2 and IEC 61508-3	2000	145 (72)
第7部	技術及び手法の概観 Overview of techniques and measures	2000	229 (100)

計 835
(計 382)

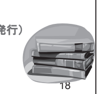
17

IEC 61508 について　(4／4)

IEC 61508 (JIS C0508) をベースとした分野別規格

1. IEC 62279 (2003)　鉄道用 (ソフトの規定有り)
   Railway applications
   – Communications , signalling and processing systems –
   Software for railway control and protection systems
2. IEC 61513 (2001)　原子力
3. IEC 61511 (2003)　プロセス産業
4. IEC 61800 (2003)　電動モータ
5. IEC 62061 (2005)　産業機械
6. ISO 26262 (2011)　自動車(2009年6月DIS発行)

等々



18

機能安全の定義

●機能安全とは、
絶対的な安全を確保する「本質安全」という概念とは異なり、安全度水準を設定して、リスクの評価を行い、許容リスク以下になるようにリスク軽減を実施するという考え方。(経産省 情報処理振興課 産業構造審議会資料 '06-12-14)

本質安全：システムの設計又は運転特性に向けられた概念(固有安全)
機能安全：安全に寄与する保護システム、保護機能に向けられた概念

絶対安全(リスク 0)は、ありえない。相対的に安全であるにすぎない。(ISO/IEC指針51)

従って、定量的な尺度によって、安全度合を決める必要がある。

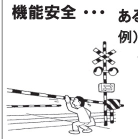
→ 安全度水準 (SIL : Safety Integrity Level)

19

本質安全と機能安全

本質安全 ・・・ 根源からリスクをなくして達成する安全のこと。
例)踏切事故をなくすために立体交差にする。

機能安全 ・・・ ある機能によって確保される安全のこと。
例)踏切、信号、列車停止装置などの周辺の安全関連系によってリスクを軽減する。

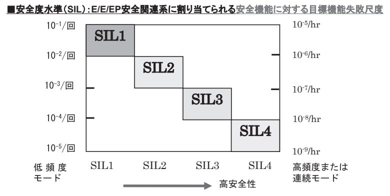


20

安全度水準　(SIL)

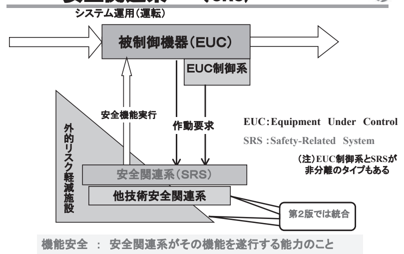
IEC61508 では、システムに求められる目標とする安全機能が、どの程度の割合で機能不全にいたるかの許容度を4つの水準に区分しており、これを「安全度水準」(Safety Integrity Level; SIL)と呼んでいる。

■安全度水準(SIL)：E/E/EP安全関連系に割り当てられる安全機能に対する目標機能失敗尺度



21

安全関連系　(SRS)



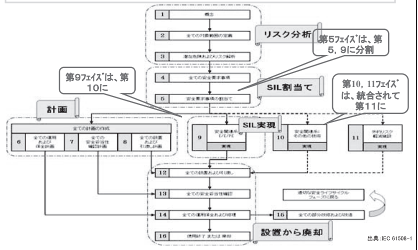
EUC : Equipment Under Control
SRS : Safety-Related System
(注)EUC制御系とSRSが非分離のタイプもある

機能安全 : 安全関連系がその機能を遂行する能力のこと
SIL : その能力の失敗確率で安全度を評価する

22

全安全ライフサイクル　(第1版)

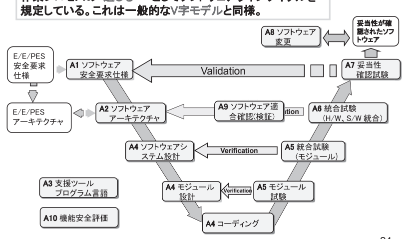
安全度水準を満足する安全関連系を実現するための道標として「全安全ライフサイクル」を規定し、リスク分析、設計から、運用、保守、廃棄に至るまでの規範手順を示している。



出典：IEC 61508-1

ソフトウェア開発ライフサイクル

作業プロセスの"道しるべ"としてソフトウェアライフサイクルを規定している。これは一般的なV字モデルと同様。



24

安全のお手本

ソフトウェアの設計・開発の各作業段階において、用いるべき技術や手法(ベストプラクティス)が示されており、目標とする安全度水準(SIL)に応じて適用することが要求されている。

IEC 61508-3 表A.2 ソフトウェアアーキテクチャにおけるベストプラクティスと推奨指針(抜粋)

技術／手法	SIL 1	SIL 2	SIL 3	SIL 4
人工知能による障害是正	–	×	×	×
構造化手法	◎	◎	◎	◎
有限状態機械/状態遷移図	○	○	◎	◎
時間ペトリネット	○	○	◎	◎
決定表(真理値表)	○	○	◎	◎
形式的手法(数学モデル等による仕様の検証)	–	○	○	◎
コンピュータ支援による仕様書作成ツール	○	○	◎	◎

・技法が多い(約100)
・条件も複雑

–：推奨なし
○：推奨(R)
◎：強い推奨(HR)
×：非推奨(NR)

25

推奨技法：適切なプログラム言語

表 C.1 – 個々のプログラミング言語に関する勧告

	プログラミング言語	SIL1	SIL2	SIL3	SIL4
1	ADA	HR	HR	R	R
2	サブセット付き ADA	HR	HR	HR	HR
3	MODULA-2	HR	HR	R	R
4	サブセット付き MODULA-2	HR	HR	HR	HR
5	PASCAL	HR	HR	R	R
6	サブセット付き PASCAL	HR	HR	HR	HR
7	FORTRAN 77	R	R	R	R
8	サブセット付き FORTRAN 77	HR	HR	HR	HR
9	C	R	–	NR	NR
10	サブセット及びコーディング基準を持ち，また静的解析ツールを用いる C	HR	HR	HR	HR
11	PL/M	R	–	NR	NR
12	サブセット及びコーディング基準をもつ PL/M	HR	R	R	R
13	アセンブラ	R	R	–	–
14	サブセット及びコーディング基準をもつアセンブラ	R	R	R	R
15	ラダーダイアグラム	R	R	R	R
16	言語の定義されたサブセットをもつラダーダイアグラム	HR	HR	HR	HR
17	機能ブロックダイアグラム	R	R	R	R
18	言語の定義されたサブセットをもつ機能ブロックダイアグラム	HR	HR	HR	HR
19	構造化テキスト	R	R	R	R
20	言語の定義されたサブセットをもつ構造化テキスト	HR	HR	HR	HR
21	順次機能チャート	R	R	R	R
22	言語の定義されたサブセットをもつ順次機能チャート	HR	HR	HR	HR
23	命令リスト	R	–	NR	NR
24	言語の定義されたサブセットをもつ命令リスト	HR	R	R	R

26

IEC 61508 の課題

1. 膨大な規格であり、すべてを理解するのは至難。
2. 情報セキュリティ、ヒューマンエラーは、扱い少。
3. ベストプラクティスは、技法の列挙。
   (分野別の規格が整備されるか安全設計の基礎知識がないと対処が難しい)

27

ISO 26262 の概要 (1/3) Road vehicles—Functional safety—

規格全体構成　ISO/DIS 26262 より抜粋

ISO 26262 の概要　(2/3)

Road vehicles—Functional safety—

規格書の構成

1. 用語
2. 機能安全マネジメント
3. コンセプトフェーズ
4. 製品開発 ： システム
5. 製品開発 ： ハードウェア
6. 製品開発 ： ソフトウェア
7. 生産と運用
8. 支援プロセス
9. ASILと安全指向の解析
10. ガイドライン(参考)

(3.～7.) コアプロセス

29

ISO 26262 の概要　(3/3)

IEC 61508との対比

1. SILとASILの違い

ASIL : A　B　C　D
SIL : 1　2　3　4

2. 規格制定の背景の相違

IEC 61508 : 分野を特定せず。据付型設備には適合しやすい。
ISO 26262 : 自動車分野に特定。量産品向け。

30

第三者認証機関について

■ 国際機能安全規格 IEC61508 の第三者認証を発行している機関は日本にはまだ無く、ドイツなどの認証機関に依頼する例が多い。

■ 機能安全規格の第三者認証機関としては、テュフズードジャパン株式会社 と テュフラインランドジャパン株式会社などが日本で活動している。

注：
テュフ(TÜV)とは、ドイツ語 "Technischer Überwachungs Verein" の頭文字をとったもので、技術検査協会と いう意味。

31

IEC61508認証取得プロセス概要

- フェーズ0 教育(セミナー、ワークショップ、テクニカル・ミーティングによる準備)
- フェーズ1 安全に関する基本計画、安全要求仕様の確認、FSM*の監査(Audit)　約2週間
- フェーズ2 H/W、S/Wドキュメントレビュー、FMEAのレビュー、安全ライフサイクルの監査　約5週間
- フェーズ3 危険側故障、安全機能の失敗確率の計算、故障モードの解析　約2週間
- フェーズ4 電磁波ノイズテスト、電気的安全性テスト、環境テスト　約4週間以上
- フェーズ5、6 ドキュメント体系、工場の検査　約1週間
- フェーズ7 テストレポート作成、認証作業　約1ヶ月

最短半年～2年以上

*FSM : Functional Safety Management

32

Ⅱ. 組込みシステムにおける安全設計

1. 組込みシステムの状況
2. 安全に対する関心の高まり
3. 機能安全規格の概要
4. **安全に関する用語と概念の整理**
5. ソフトウェアの安全設計

・安全性と信頼性
・セキュリティとセーフティ
・リスクとは
・障害と故障
・停止の概念
・ハードとソフトの違い

33

安全に関する用語の定義

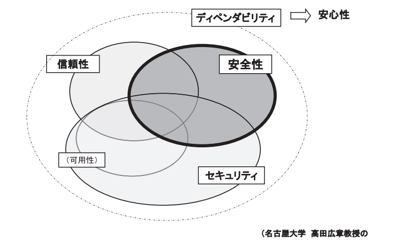
(ISO/IEC Guide 51(JIS Z 8051) : 1998)

用語	概要
安全 (Safety)	受容できないリスクがないこと。
リスク (risk)	危害の発生確率及びその危害の程度の組合せ。
危害 (harm)	人の受ける身体的傷害若しくは健康傷害、又は財産若しくは環境の受ける害。
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。
ハザード (hazard)	危害の潜在的な源。
危険状態 (hazardous situation)	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況。
許容可能なリスク (tolerable risk)	社会における現時点での評価に基づいた状況下で受け入れられるリスク。
保護方策 (protective measure)	リスクを低減するための手段。
残留リスク (residual risk)	保護方策を講じた後にも残るリスク。

＊ JASAの用語集サイト : http://jasa.or.jp/sa/yougosyu.html

34

安全性に係わる概念



(名古屋大学 高田広章教授の ET2008講演(TD-1)より。一部修正)

35

安全性と信頼性　(JIS Z8115の定義)

ソフトウェアはハードウェアのような経年劣化故障がないこともあって、特に、安全性と信頼性は、混同されやすい。

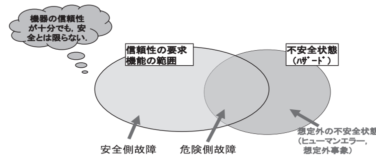
◆安全性：人への危害または損害の危険性が、許容可能な水準に抑えられている状態

◆信頼性：機器、設備などのアイテムが与えられた条件のもとで、与えられた期間、要求機能を遂行できる能力

品質の役割と安全の役割とを混同しないこと (ISO/IEC指針51)

36

安全性と信頼性　(イメージ的差異)

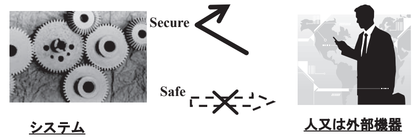


安全側故障 → 機械が壊れても安全が保たれる。
危険側故障 → 機械が壊れると安全が保証されない。
想定外の不安全状態 → 機械が正常でも安全が保証されない。

37

セキュリティ と セーフティ

どちらも和訳は「安全」だけど、、、、



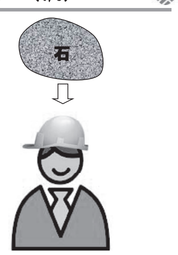
セキュリティ	： 危害を(外部から)及ぼされない
セーフティ	： 危害を(外部へ)及ぼさない

38

リスクとは、　(1/3)

ヘルメットの例

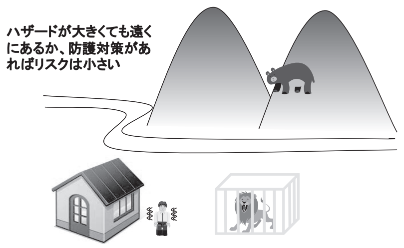
安全ヘルメットをつけていれば安全と言うわけではない。単に頭を一定の力から保護しているにすぎない。



39

リスクとは、　(2/3)

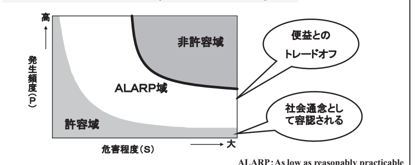
ハザードが大きくても遠くにあるか、防護対策があればリスクは小さい



40

リスクとは、　(3/3)

◆部品やシステムが持つ潜在的な危険性
◆リスク ＝ 発生頻度(P)×危害の程度(S)



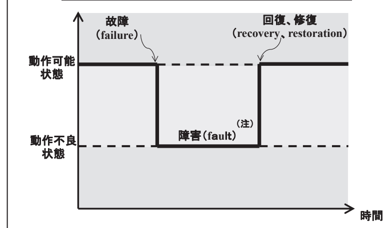
ALARP : As low as reasonably practicable

☆ リスクは、いたる処に存在するが、正確に認識されていることは少ない。
リスク評価を行い、許容範囲に抑えることが、重要。

41

障害 と 故障　(1/3)

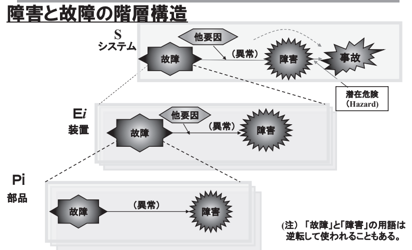
JIS Z8115(2000)の解説を時間軸で表現すると。



(注 : JIS Z8115 は「障害」とは言わず「フォールト」と言っている)　42

障害 と 故障　(2/3)

障害と故障の階層構造



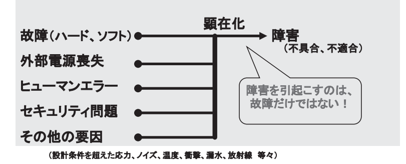
(注) 「故障」と「障害」の用語は逆転して使われることもある。

43

障害 と 故障　(3/3)

障害の要因

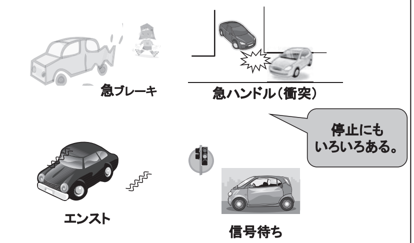
◆障害(Fault) ： 要求機能を実行できない状態 (不具合)
◆故障(Failure) ： 要求機能を実行する能力がなくなる事象
(なお、安全設計では、安全側故障と危険側故障に大別する)



(設計条件を超えた応力、ノイズ、温度、衝撃、漏水、放射線 等々)

44

停止の概念　(1/2)　車の例

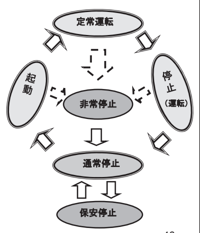


45

停止の概念　(2/2)　プラントの例

- 通常停止
  - ・通常手動停止
  - ・通常自動停止
- 非常停止（緊急停止）
  - ・非常手動停止
  - ・非常自動停止
- 保安停止（隔離停止）
  - ・手動
- 制御停止（待機状態）
  - ・手動
  - ・自動
- 故障停止
- その他の停止

発電プラントの運転フェイズ



46

ハードとソフトの違い

◆ハードウェア
- ・劣化する 。
- ・故障は偶発的に発生する（ランダム故障）。
- ・性能がドリフトする 。

⇒ *品質改善は統計的に評価*

◆ソフトウェア
- ・基本的に劣化しない（ 陳腐化する）。
- ・故障の要因は決定論的原因故障。
  （設計、製造時に作りこむ不適合）である。

⇒ *品質改善はプロセスを評価*

安全要求事項も異なってくる。

47

ソフトウェアの安全性とは？

ソフトウェアの機能安全

ソフトウェアに対して故障確率を考えることは出来ない。

IEC 61508 では、ライフサイクルの作業ステージ毎に、SIL に応じて実現すべき技法・手法を設定している。これらの技法・手法を確かに実現していれば、その安全度水準（SIL）に達しているとみなされる（プロセスを評価）。

48

Ⅱ. 組込みシステムにおける安全設計

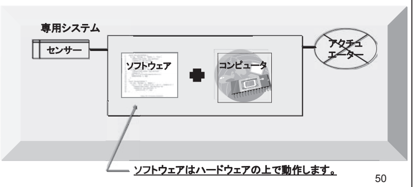
1. 組込みシステムの状況
2. 安全に対する関心の高まり
3. 機能安全規格の概要
4. 安全に関する用語と概念の整理
5. ソフトウェアの安全設計
   （システムの安全設計）

- ・システム視点での準備
- ・リスク評価
- ・設計戦略、基本手法
- ・ケーススタディ
- ・実力評価
- ・開発プロセスの整備
- ・認証対策

49

システムの視点

✓ ソフトウェアは単独では動作しない。そのため、ソフトウェア単独で安全性を議論することはできず、システムとして安全性を考える必要がある。



50

ハードとソフトの違い（機能安全の実現）

システムの安全性確保にあたってはハードウェアとソフトウェアの故障特性を知って適切に対応することが重要。

☆ハードウェア　：確率論的故障（random hardware failure）
経年劣化によって偶発的に発生する故障。

対策
- ・部品の寿命管理
- ・ハードウェアの冗長化、危険側故障の低減
- ・ソフトウェアによる監視・診断機能構築　などで対応

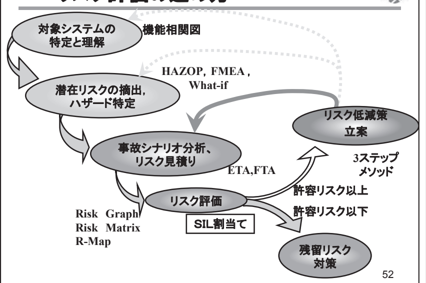
☆ソフトウェア　：決定論的故障（systematic failure）
設計、製造時の不適合によって発生する故障。　特に変更管理

対策
- ・開発プロセスの的確な管理と適切な分担組織
- ・安全要求仕様の明確化
- ・適切な技法・手法の採用、SPL化　などで対応

SPL: Software Product Line

51

リスク評価の進め方



52

主なリスクアセスメント技法

技法	概要
What-if	非体系的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。
FMEA Failure Mode and Effect Analysis	製品および製造プロセスについて故障モードによる影響を分析して製品やプロセスの問題を解決する手法である。製品が使用される段階で起こりうる欠陥や異常な状態などを分析する。
HAZOP Hazard and Operability Study	通常状態からのズレ（設定の温度や濃度）が発生した場合にその原因と発生する結果の事象を特定する。
FTA Fault Tree Analysis	システムの特定故障を想定して、その発生原因を上位レベルから下位レベルまで論理的に展開し、最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める方法である。
ETA Event Tree Analysis	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。
Risk Graph	ツリー形式で示される方法で、想定される危害のひどさ、危険源／危険事象／危険状態にさらされる頻度、回避の可能性などがリスクパラメータとなる。
Risk Matrix	危害の発生頻度と危害のひどさを定性的に見積る手法である。それぞれの要素の分類は4分類する場合や6分類する場合など任意である。
R-Map	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。それにより対象製品を客観的な視点、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）日科技連が推進している。

53

安全設計の基本手法（3ステップメソッド）

安全設計の3ステップメソッド　（案外、知らない人が多い。）

(1)ステップ1：本質的安全設計方策

(2)ステップ2：安全防護策（機能的安全設計策）

(3)ステップ3：使用上の情報

SIL-3 取得製品を活用してもいい

54

主な安全設計技法

技法	概要
ゼロメカニカルステート（ZMS）設計	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
フェールセーフ設計	故障が発生しても安全側になるよう配慮した設計
フールプルーフ設計	人の不適切な行為、過失があっても安全性が損なわれないように配慮した設計。 チャイルドプルーフ、タンパープルーフ、ミスティクプルーフ等も考え方は同じ。
ツーハンドコントロール	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。安易な操作を避ける。
冗長設計	システムの構成要素や機能の実現手段を複数用意し、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。
ディレーティング	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こと
防御的プログラミング	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

55

主な安全設計戦略

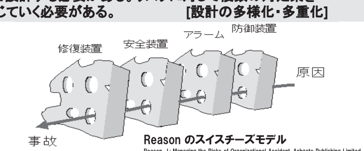
- フォールト アボイダンス、フォールト レジスタンス
  （障害を回避、抵抗力を高める仕組み）
- フォールト トレランス
  （障害発生に対し許容性を持たせる仕組み）
- フォールト ディテクション
  （障害検出→安全性確保のトリガー、復旧対応）
- 深層防護、多重防護
  （発生防止→拡大抑制→影響緩和）

56

安全性の確保　（多重防護の思想）

◆安全性の確保は、単に品質を管理するだけでは、難しい。システムのライフサイクル全体に渡って（廃却まで！）、多重に整備していく必要がある。　[管理の多重化]

◆安全性の確保は、常に想定外の事態が発生することを想定して設計する必要がある。リスクに対して複数の対処策を講じていく必要がある。　[設計の多様化・多重化]



Reason のスイスチーズモデル
Reason, J.: Managing the Risks of Organizational Accident. Ashgate Publishing Limited. 1997

57

ケーススタディ（失敗事例に学ぶ　1/2）

失敗事例に学ぶ（課題例）

オートマチック車（AT車）のエンジンをかけたところ、異常な音をたてて、通常は1,000回転以下のところが 3～4,000回転にもなった。ギヤが入っていれば大事故につながる。
原因は、コンピュータの集積回路（IC）のはんだづけ部分にき裂が入り、電気が通じ難くなったため、コンピュータが誤作動し、スロットルバルブを勝手に開き、エンジンが高速回転になった為とわかった。
（出典：JST）

失敗データベース（http://shippai.jst.go.jp/fkd/Search）

58

ケーススタディ（失敗事例に学ぶ　2/2）

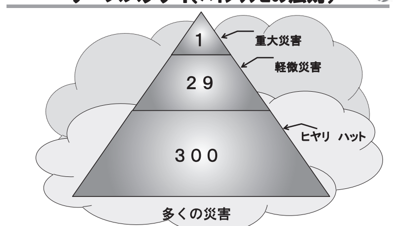
失敗事例に学ぶ（何が問題か？）

前記の事例に対してグループで議論することにより、安全に対する関心・感覚を養成していく。

- ✓ 検討すべき障害の範囲はどうやって決めるか？
- ✓ 障害検出はどこまで可能か？
- ✓ 担当者の知識・経験不足はどうやってカバーするか？

59

ケーススタディ（ハインリッヒの法則）



重大災害の裏には、300以上のヒヤリハットがある。
小さなトラブル事例も分析・真因追及することが重要。

60

ケーススタディ（制御用計算機に学ぶ）

ハード故障により、ソフトが正しく動かないリスクを想定していた。

制御用計算機システムの安全確保策事例

- ・自動再起動機能
- ・システムコールのミニマム化
- ・HDDアクセス最小化
- ・監視系は、多重化と多層チェック。
- ・制御系は、半形式手法による表記。
- ・解析・記録系は、ダイバーシティ化。
- ・その他

等々

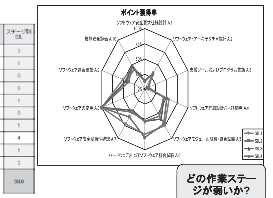
61

ツールによる実力診断（現状の定量的評価）

ソフトウェアに要求されたSIL（安全度水準）への適合度を数値として可視化する。どの部分が不十分か明確にする。

◆ ステージ別評価結果

NO	評価対象	ステージ別SIL
A1	ソフトウェア安全要求仕様設計	2
A2	ソフトウェア・アーキテクチャ設計	1
A3	支援ツールおよびプログラム言語	0
A4	ソフトウェア詳細設計および開発	0
A5	ソフトウェアモジュール試験・統合試験	1
A6	ハードウェアおよびソフトウェア統合試験	0
A7	ソフトウェア安全妥当性確認	1
A8	ソフトウェアの変更	4
A9	ソフトウェア適合確認	1
A10	機能安全評価	2
	総合結果	SIL0



どの作業ステージが弱いか？

"安診太郎"による評価結果例

62

開発プロセスの整備

【開発プロセス管理】
品質・信頼性の作り込み管理に使用する品質管理工程図（QCP：Quality Control Process Chart）に安全視点を追加し、品質管理と併せて安全設計管理を実施する。

ESPR Ver.2.0
◆組込みソフトウェア向け開発プロセスガイド
IPA／SEC（独立行政法人　情報処理推進機構）編著

安全文化の確立

安全設計は組織への安全思考の定着が重要。そのためには、各々の組織に合った安全視点のQCPを確立する必要がある。

63

認証対策

安全規格認証取得策

1. ハザード、リスクを明確にしておく。
2. 対象製品の構成要素を安全系と非安全系に分離し、安全関連系を特定（限定）する。
3. 安全系にSIL3取得済みの部品・製品を利用して、認証対象をさらに絞り込む。
4. ドキュメントを整備する。
5. エビデンスを整備・蓄積する。

64

機能安全に関する今後の課題

- 用語の不統一
- ソフトウェアの安全設計はまだ未確立
  （IEC 61508は推奨手法をリストアップ）
  （手法が体系化されていない）
- 規格は欧州先行
  （日本はまだ未整備）

65

参考文献

1. 安全の国際規格　第1巻　安全設計の基本概念　2007-5
   向殿政男　監修　日本規格協会発行
2. 安全の国際規格　第3巻　制御システムの安全　2007-9
   向殿政男　監修　日本規格協会発行
3. 組込みシステムの安全性向上の勧め　2006-11
   （独法）情報処理推進機構　ソフトウェア・エンジニアリング・センター　編　オーム社雑誌局発行
4. 産総研ワークショップ　機能安全規格と適合認証　IEC61508のさらなる理解に向けて
   （独法）産業技術総合研究所　関西センター システム検証研究センター　2006-2-8
5. ネット社会における組込みシステム、2つの課題 「情報セキュリティ」と「機能安全」
   （ 平成19年度 組み込みシステムにおける機能安全に関する調査研究 ）
   （社）組込みシステム技術協会　2008-3
6. 組込み系技術者のための安全設計入門
   （ 平成20年度　組み込みシステムにおける機能安全に関する調査研究 ）
   （社）組込みシステム技術協会　2009-3
7. 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21年度　組み込みシステムにおける機能安全に関する調査研究 ）
   （社）組込みシステム技術協会　2010-3
8. 安全と安心の科学　2005-1
   村上陽一郎　集英社 （集英社新書）
9. 組込み系技術者のための安全設計入門
   （社）組込みシステム技術協会　電波新聞社　2010-5

66

ご清聴有難うございました。

JASA
安全性向上委員会
製品安全WG

お問合せ先 ：
社団法人　組込みシステム技術協会（JASA）
東京都中央区日本橋浜町1-8-2
TEL:03-5821-7973　FAX:03-5821-0444
E-mail:jasainfo@jasa.or.jp
http://www.jasa.or.jp/

67

組込みシステムの機能安全

Ⅲ．機能安全設計の基本

～ 機能安全実現のために ～

安全性向上委員会　製品安全WG
水口　大知
産業技術総合研究所

特定非営利活動法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

Ⅲ．機能安全設計の基本

水口　大知

身近な機能安全

ガスメータ、継続使用時間遮断機の不作動（’06/2）
立ち乗りスクータ、タイヤの逆転（’06/9）
埋込型心臓ペースメーカ、ペーシングの抑制（’07/2）
湘南モノレール、オーバーラン（’08/2）
自動体外式除細動器、自己診断で検出できない電子部品の故障（’09/11）

安全関連システムとIEC 61508

IEC 61508は、安全関連システムの開発・運用のガイドライン
- 「電気・電子・プログラマブル電子安全関連系の機能安全」
- 鉄道、産業機械、自動車、医療機器等の機能安全規格に影響

主な目的は、
- 安全関連システムの要求仕様において、安全機能に対し適切な安全性能目標を設定すること→*安全度*
- 安全関連システムの設計・開発および運用において、設定された安全機能の安全性能目標を、確実に達成すること→*安全ライフサイクル*

IEC 61508の考え方

機能安全 ＝ 安全機能 ＋ 安全度

安全のために何をするか
Ex）
・制御対象の安全状態を達成／維持する機能
・センサ、PEハードウェア、アクチュエータの障害を検出／制御する機能
・ソフトウェア自身の障害を検出／制御する機能

安全機能の失敗がどの程度許容されるか
・安全水準（SIL 1～SIL 4）によって規定される
Ex）SIL 3 なら、目標機能失敗尺度は、危険側故障率PFH［1/Hour］が10^{-8}～10^{-7}または
作動要求毎の機能失敗確率PFD_{avg}が10^{-4}～10^{-3}

ハザード分析により機能仕様を決定

リスクアセスメントにより安全度目標を決定

安全度
＝ ハードウェア安全度 ＋ システマティック安全度

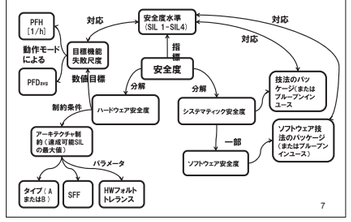
ランダムHW故障への対策の度合い
・基本的に、ハードウェア設計における機能失敗尺度の推定値が、目標値を下回ればよい
・ただし、安全側故障割合が低い場合は、ハードウェアの冗長化が必要となる

信頼性の高い部品の使用、系の多重化、共通原因故障の排除、診断テストによる故障診断率の向上、

システマティック故障への対策の度合い
・システマティック故障の回避および抑制による

安全ライフサイクルの規定、各フェースにける技法の推奨、機能安全マネジメントの導入、文書化、機能安全アセスメント、

安全度に関わる概念

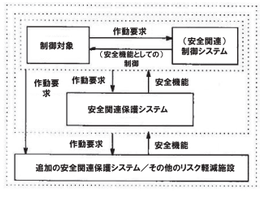


Ⅲ．機能安全設計の基本

安全関連システムとは

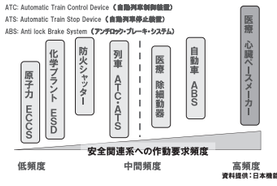
制御対象を安全な状態に導いたり、制御対象の安全な状態を維持したりする機能を担うシステム

システムの全体像



安全関連システムと作動要求頻度

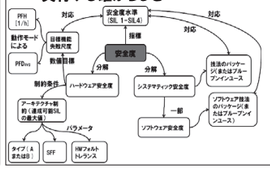
ECCS: Emergency Core Cooling System（非常用炉心冷却装置）
ESD: Emergency Shutdown System（緊急停止装置）
ATC: Automatic Train Control Device（自動列車制御装置）
ATS: Automatic Train Stop Device（自動列車停止装置）
ABS: Anti lock Brake System（アンチロック・ブレーキ・システム）



資料提供：日本機能安全

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下で、規定の安全機能を満足に実行する確からしさ

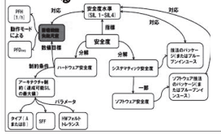


安全度水準（SIL）

安全度には4段階の水準が規定されており、SIL 1～SIL 4と表記する
- SILが高くなることは、安全関連システムが安全機能の実行に失敗する可能性が低くなることを意味する
- 4を上回るSILは規定されていない

目標機能失敗尺度（TFM）

求められる安全度に応じて達成すべき危険側故障確率の目標
- SIL が大きくなるとTFMは小さくなる
- 安全機能の運用モードによって値の単位が異なる



低頻度作動要求モードに対するTFM

SIL	作動要求時の平均危険側故障確率PFD_{avg}	（許容される危険側故障）
4	10^{-5}以上10^{-4}未満	（数万回に1回）
3	10^{-4}以上10^{-3}未満	（数千回に1回）
2	10^{-3}以上10^{-2}未満	（数百回に1回）
1	10^{-2}以上10^{-1}未満	（数十回に1回）

高頻度作動要求モード・連続モードに対するTFM

SIL	単位時間あたりの危険側故障確率（頻度）PFH［1/h］	（許容される危険側故障）
4	10^{-9}以上10^{-8}未満	（数万年に1回）
3	10^{-8}以上10^{-7}未満	（数千年に1回）
2	10^{-7}以上10^{-6}未満	（数百年に1回）
1	10^{-6}以上10^{-5}未満	（数十年に1回）

安全機能の運用モード

低頻度作動要求モード：安全機能への作動要求頻度が、年1回以下である運用モード
高頻度作動要求モード：安全機能への作動要求頻度が、年1回より大きい運用モード
連続モード：安全機能が通常運用の一部として制御対象を安全状態に維持し続けるような運用モード

「故障確率」

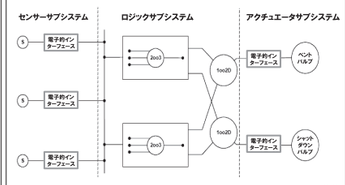
PFD_{avg}：安全関連システムが、作動要求時に所定の安全機能を遂行できない平均確率（平均アンアベイラビリティ；無次元量）
PFH：単位時間あたりの、安全関連システムの危険側故障の平均確率（平均頻度［1/Hour］）

安全関連システムの安全要求仕様

安全機能
- 制御対象の安全状態をどのように達成または維持するかの方法

安全機能の運用モード
安全機能に要求されるSIL
その他
- 応答時間性能
- 操作者とのインターフェース
- 他のシステムとのインターフェース
- 制御対象の動作モード
- 故障時の振舞いと必要となる反応
- ハードウェアとソフトウェアの間の関係や制約
- 制約事項、制限事項（時間制約など）
- 起動時および再起動時の手順に関連する事項
- プルーフテストに関する要求事項や制約
- ライフサイクルにおいて想定される極端な使用環境
- 電磁イミュニティの限界値

安全関連システムのアーキテクチャ



IEC 61508-6より抜粋

安全度の2つの側面

安全機能の安全度が損なわれる2つの原因
- ランダムハードウェア故障：物理的な劣化のメカニズムによって、ハードウェアにおいてランダムに生じる故障
- システマティック故障：設計や製造、運用における特定の誤りが原因となって、決定論的に生じる故障
  - システマティック故障の原因例
    - ✓ 安全関連系の安全要求仕様における誤り・抜け
    - ✓ ハードウェアまたはソフトウェアの要求仕様の誤り・抜け
    - ✓ ハードウェアの設計誤り
    - ✓ ソフトウェアバグ
    - ✓ ヒューマンエラー（設計不備に起因したエラー）
    - ✓ 保守・修正手順の不備

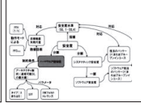
安全度＝ハードウェア安全度 and システマティック安全度

Ⅲ．機能安全設計の基本

ハードウェア安全度の達成

ハードウェア設計における機能失敗尺度の推定値が、リスクアセスメントの結果として安全関連系に割り当てられた目標機能失敗尺度を下回ればよい

推定は、FTA、信頼性ブロック図、マルコフモデル、ペトリネットなどによる



機能失敗尺度推定のためのパラメータ

パラメータ	意味
T_1	プルーフテスト間隔
λ_{DU}	チャネルのDU故障率（診断テストにより自動検出できない危険側故障）
λ_{DD}	チャネルのDD故障率（診断テストにより自動検出できる危険側故障）
DC	チャネルの診断率 DD故障率 λ_{DD}=DC λ_D、 DU故障率 λ_{DU}=（1-DC） λ_D
β	診断テストにより自動検出できない故障のうちで共通原因をもつ故障の割合
β_D	診断テストにより自動検出できる故障のうちで、共通原因をもつ故障の割合
MTTR	平均修復時間（Mean Time To Restoration）

安全関連システムのハードウェア故障分類

	診断できる	診断できない
安全側	自己診断可能な安全側故障	自己診断不能な安全側故障
危険側	自己診断可能な危険側故障（DD故障）	自己診断不能な危険側故障（DU故障）

パラメータの決定

故障率 λ_{DU}、λ_{DD}
- FMEDAにより決定

診断率DC
- 用いる診断技法により決定

共通原因故障割合 β の決定
- チェックリストの得点により決定

DCの規定例

ROMに対する診断技法

診断技法	達成可能な最大の自己診断率
多重ビットによる冗長化	Medium
チェックサム	Low
1ワード（8ビット）のシグニチャ	Medium
2ワード（16ビット）のシグニチャ	High
ブロックの複製	High

Low:60%、Medium:90%、High:99%

処理ユニットに対する診断技法

診断技法	達成可能な最大の自己診断率
コンパレータ	High
多数決	High
ソフトウェアによる自己試験：制限された数のパターン（1チャネル）	Low
ソフトウェアによる自己試験：ウォーキングビット（1チャネル）	Medium
ハードウェア支援による自己試験（1チャネル）	Medium
コード付処理	High
ソフトウェアによる相互比較	High

Low:60%、Medium:90%、High:99%

ハードウェア安全度のアーキテクチャ制約

エレメントの「タイプ」、「安全側故障割合：SFF」および「ハードウェアフォルトトレランス」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

以下を満たすエレメントがタイプA（それ以外はタイプB）
- 全ての構成要素の故障モードを十分定義できる
- 障害条件下のエレメントの挙動を完全に決定できる
- 主張される故障率を裏付けるために十分信頼できる故障データがある

SFF = （$\lambda_S + \lambda_{DD}$）/（$\lambda_S + \lambda_D$）
ハードウェアフォルトトレランス = 多重化の度合い

タイプAのサブシステムにより遂行される安全機能に対して割当てることのできる最大SIL

チャネルのSFF	ハードウェアフォルトトレランス		
	0	1	2
SFF＜60%	SIL 1	SIL 2	SIL 3
60% ≦SFF＜90%	SIL 2	SIL 3	SIL 4
90% ≦SFF＜99%	SIL 3	SIL 4	SIL 4
99% ≦SFF	SIL 3	SIL 4	SIL 4

31

タイプBのサブシステムにより遂行される安全機能に対して割当てることのできる最大SIL

チャネルのSFF	ハードウェアフォルトトレランス		
	0	1	2
SFF＜60%	許可されない	SIL 1	SIL 2
60% ≦SFF＜90%	SIL 1	SIL 2	SIL 3
90% ≦SFF＜99%	SIL 2	SIL 3	SIL 4
99% ≦SFF	SIL 3	SIL 4	SIL 4

32

Ⅲ. 機能安全設計の基本

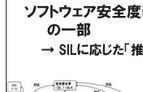
33

システマティック安全度の達成

安全関連システムの開発および運用における誤りの混入を防ぐことにより、システマティック故障の発生を回避(Avoid)する

安全関連システムの運用中にシステマティック故障が発生してしまった場合にその影響を抑制(Control)する

→ SILに応じた推奨技法の「パッケージ」を規定



34

システマティック故障を回避すべきフェーズ

E/E/PEシステム設計要求の仕様策定

E/E/PEシステム設計および開発

E/E/PEシステム統合

安全関連システムの運用および保全

安全関連システムの安全妥当性確認

35

E/E/PEシステム設計要求の仕様策定における誤り回避のための推奨技法

	技法	SIL 1	SIL 2	SIL 3	SIL 4
	プロジェクト管理	M low	M low	M medium	M high
	文書化	M low	M low	M medium	M high
	安全機能とそうでない機能の分離	HR low	HR low	HR medium	HR high
	構造化された仕様記述	HR low	HR low	HR medium	HR high
	仕様のインスペクション	– low	HR low	HR medium	HR high
	準形式手法	R low	R low	HR medium	HR high
	チェックリスト	R low	R low	R medium	R high
	コンピュータ支援の仕様記述ツール	– low	R low	R medium	R high
	形式手法	– low	– low	R medium	R high 36

影響を抑制すべきシステマティック故障

ハードウェアの設計における誤り

環境負荷

制御対象のオペレータによる誤り

ソフトウェア設計における残存誤り

データ通信エラー

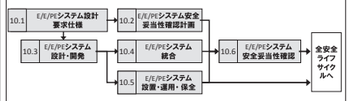
37

ハードウェア設計誤りに起因するシステマティック故障の抑制のための推奨技法

	技法	SIL 1	SIL 2	SIL 3	SIL 4
	プログラムシーケンス監視	HR low	HR low	HR medium	HR high
	オンライン監視による故障検出	R low	R low	HR medium	HR high
	冗長なハードウェアによるテスト	R low	R low	HR medium	HR high
	標準的なテストアクセスポートおよびバウンダリスキャンアーキテクチャ	R low	R low	R medium	R high
	コードの保護	R low	R low	R medium	R high
	ハードウェアの多様化	– low	– low	R medium	R high

38

E/E/PEシステム安全ライフサイクル



39

システマティック故障と目標機能失敗尺度

システマティック故障の回避・抑制に関する要求事項は、「エキスパートジャジメント」であり、これらを全て満たすことによって、ハードウェア安全度と同等のシステマティック安全度が達成されたと主張することを認めるものである

このことは、IEC 61508が要求事項を展開する上での大前提となっている

40

Ⅲ. 機能安全設計の基本

41

安全関連ソフトウェアの開発

安全関連ソフトウェアによる実現を考慮すべき機能は：

- 制御対象における安全状態の達成または維持を可能とする機能
- プログラマブル電子装置ハードウェアや、センサー、アクチュエータの異常を検出して対処する機能
- ソフトウェア自身の異常を、検出して対処するための機能
- 安全機能の周期テストに関連する機能
- 安全関連システムを安全に修正するための機能

42

ソフトウェア安全度

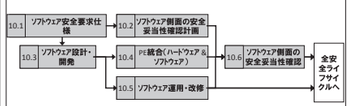
システマティック安全度のうち、ソフトウェアに起因するシステマティックな危険側故障に関連する部分

ソフトウェア安全度は、システマティック安全度の一部

→ SILに応じた「推奨技法のパッケージ」による

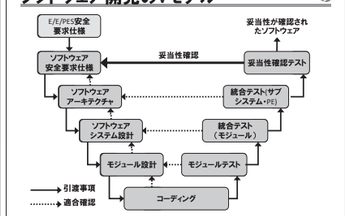
43

ソフトウェア安全ライフサイクル



44

ソフトウェア開発のVモデル



45

ソフトウェアアーキテクチャ設計における推奨技法

	技法	SIL 1	SIL 2	SIL 3	SIL 4
1	フォールトの検出	–	R	HR	HR
2	エラーを検出するコード	R	R	R	HR
3a	故障を表明するプログラミング	R	R	R	HR
3b	多様な監視技術(監視機能と被監視機能が同一コンピュータ上にあって独立している)	–	R	R	–
3c	多様な監視技術(監視コンピュータと被監視コンピュータが分離している)	–	R	R	HR
3d	多様な冗長化(同じソフトウェア安全要求仕様を実装するもの)	–	–	–	R
3e	機能的に多様な冗長化(異なるソフトウェア安全要求仕様を実装するもの)	–	–	R	HR
3f	後方への/力バリー	R	R	–	NR
3g	状態をもたないソフトウェア設計(または制限された状態設計)	–	–	R	HR
4a	再実行によるフォールト回復機構	R	R	–	–
4b	適切な機能劣化	R	R	HR	HR
5	人工知能－フォールトの修正	–	NR	NR	NR
6	動的な再構成	–	NR	NR	NR

46

ソフトウェアアーキテクチャ設計における推奨技法(つづき)

	技法	SIL 1	SIL 2	SIL 3	SIL 4
7	モジュラアプローチ	HR	HR	HR	HR
8	信頼できる／検証されたソフトウェアエレメントの使用(利用可能な場合)	R	R	HR	HR
9	ソフトウェア安全要求仕様とソフトウェアアーキテクチャの間の助向的トレーサビリティ	R	R	HR	HR
10	ソフトウェア安全要求仕様とソフトウェアアーキテクチャの間の逆向きトレーサビリティ	R	R	HR	HR
11a	構造化された提示手法	HR	HR	HR	HR
11b	準形式手法	R	R	HR	HR
11c	形式的な設計および詳細化手法	–	R	R	HR
11d	ソフトウェアの自動生成	R	R	R	R
12	コンピュータ支援の仕様記述および設計ツール	R	R	HR	HR
13a	周期的な振舞い(最大周期時間が保証されるもの)	R	HR	HR	HR
13b	時間トリガアーキテクチャ	R	HR	HR	HR
13c	イベント駆動(最大応答時間が保証されるもの	R	HR	HR	–
14	静的な資源割り当て	–	R	HR	HR
15	共有資源へのアクセスの静的な同期	–	–	R	HR

47

(参考)ソフトウェアアーキテクチャ設計における推奨技法(第1版)

	技法	SIL 1	SIL 2	SIL 3	SIL 4
1	フォールトの検出および診断	–	R	HR	HR
2	エラーを検出して修正するコード	R	R	R	HR
3a	故障を表明するプログラミング	R	R	R	HR
3b	安全バッグ	–	R	R	R
3c	プログラミングの多様化	R	R	R	HR
3d	リカバリーブロック	R	R	R	R
3e	後方への/力バリー	R	R	R	R
3f	前方への/力バリー	R	R	R	R
3g	再実行によるフォールト回復機構	R	R	R	HR
3h	実行済みケースの記憶	–	R	R	HR
4	適切な機能劣化	R	R	HR	HR
5	人工知能－フォールトの修正	–	NR	NR	NR
6	動的な再構成	–	NR	NR	NR
7a	構造化手法(例えば、JSD、MASCOT、SADT、Yourdon等)	HR	HR	HR	HR
7b	準形式手法	R	R	HR	HR
7c	形式手法(例えば、CCS、CSP、HOL、LOTOS、時相論理、VDM、Z等)	–	R	R	HR
8	コンピュータ支援の仕様記述ツール	R	R	HR	HR

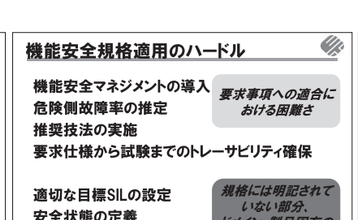
48

支援ツールおよびプログラミング言語における推奨技法

	技法	SIL 1	SIL 2	SIL 3	SIL 4
1	適切なプログラミング言語	HR	HR	HR	HR
2	強く型付けされたプログラミング言語	HR	HR	HR	HR
3	プログラミング言語のサブセット化	–	–	HR	HR
4a	認証されたツールおよびトランスレータ	R	HR	HR	HR
4b	使用実績のあるツールおよびトランスレータ	HR	HR	HR	HR

49

安全度のまとめ



50

Ⅲ. 機能安全設計の基本

51

IEC 61508 第2版での改訂のポイント

サブシステム・エレメントの定義の追加

HW安全度のアーキテクチャ制約の適合ルート追加

- 従来の要件(ルート1_H)の他に、ルート2_Hを規定

システマティック安全度の適合ルート追加

- 従来の要件(ルート1_S、ルート2_S)の他に、ルート3_Sを規定(既存ソフトウェアに対する要件)

52

Systematic Capability／エレメントの統合の導入

- エレメントに対しては、SILではなくSCを使う(ソフトウェアを含む)
- SC 1のエレメントの統合を、SC 2のエレメントとみなすことができる

53

セキュリティに関する要求事項の追加

E/E/PES安全要求仕様の分割

- E/E/PEシステム安全要求仕様(第1部)およびE/E/PEシステム設計要求仕様(第2部)に分割

データ通信に対する要求事項の詳細化

- ホワイトチャネル／ブラックチャネル

機能安全マネジメントに対する要求事項の整理

- 作業者のコンピテンシが規範要求となった

54

適合アイテムの安全マニュアルに対する要求事項の明記

ASICの設計・開発に対する要求事項の追加

no part failure/no effect failureの定義追加

- SFFの計算から除外される

55

支援ツールのクラスの導入

- T1/T2/T3

「システマティック安全度のための性質」を示す表の導入

- 「技法」により達成すべき「性質」、達成方法、厳格度を並べたもの(第3部附属書C)

56

「単一コンピュータ上でソフトウェアエレメント間の非干渉を達成するための技術」を追加

- 第3部附属書F (informative)

「安全関連オブジェクト指向ソフトウェアの開発のためのガイダンス」を追加

- 第7部附属書G (informative)

※変更箇所の確認には、"Redline version"が便利

57

Ⅲ. 機能安全設計の基本

58

機能安全規格適用のハードル

機能安全マネジメントの導入

危険側故障率の推定

推奨技法の実施

要求仕様から試験までのトレーサビリティ確保

要求事項への適合における困難さ

適切な目標SILの設定

安全状態の定義

安全機能の仕様

安全関連部の特定・分離・最小化

規格には明記されていない部分、ドメイン・製品固有の困難さ

59

ご清聴有難うございました。

JASA
安全性向上委員会
製品安全WG

お問合せ先：
社団法人 組込みシステム技術協会(JASA)
東京都中央区日本橋浜町1-8-2
TEL:03-5821-7973 FAX:03-5821-0444
E-mail:jasainfo@jasa.or.jp
http://www.jasa.or.jp/

60

組込みシステムの機能安全

IV. 機能安全の将来動向と教育体系

～ 機能安全実現のために ～

安全性向上委員会 製品安全WG

兼本 茂

会津大学 教授

組込みシステム技術協会 Japan Embedded Systems Technology Association

1

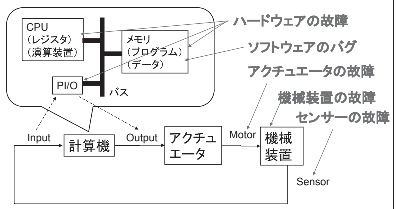
IV. 機能安全の将来動向と教育体系

1. 複雑システムのリスクアセスメントと安全設計
2. 認証のためのツール
3. 機能安全の教育

兼本 茂

2

組み込みシステム

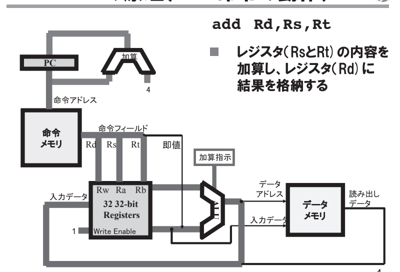


3

CPUの原理（ADD命令の動作）

add Rd,Rs,Rt

- レジスタ（RsとRt）の内容を加算し、レジスタ（Rd）に結果を格納する



4

何故組込みシステム？

- 便利で安い
  - いろんな機能を簡単に実現←ソフトウェアの便利さ
  - ハードの低価格化←たくさん作れば安くできる
  - 電子回路で作るよりずっと簡単！
- 危なくないの？
  - 機械装置とコンピュータの組み合わせで複雑化
  - 長期間使って大丈夫←機械とコンピュータでライフサイクルが異なる？
  - ソフトウェアにバグは無いの？
  - 操作ミスで危険になることは？
  - ネットワークにつなげても大丈夫？

5

組込みシステムと機能安全

- 組込み技術は、便利で安い
  - いろんな機能を簡単に実現←ソフトウェアの便利さ
  - ハードの低価格化←たくさん作れば安くできる
  - 電子回路で作るよりずっと簡単！
- 危なくないの？ →「機能安全」規格で安全を守る
  - 機械装置とコンピュータの組み合わせで複雑化→リスクアセスメント
  - 長期間使って大丈夫→信頼性解析
  - ソフトウェアのバグ→コーディング規約、形式手法
  - 操作ミスで危険になる→人間工学
  - ネットワークにつなげても大丈夫→セキュリティ対策

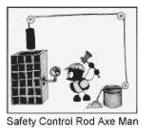
6

規格 vs 安全性原理

7

安全性の原理 ー ①フェイル・セーフ

- 停止安全が可能な場合
- 故障時に安全側に動作する



原子炉緊急停止/スクラムの語源

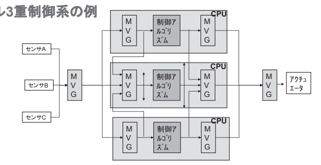
ハイボールの語源/明治大向殿教授著書

8

安全性の原理 ー ②フォールト・トレランス

- 停止安全不可の場合（飛行機、原子力、車などの複雑系）
- 多重化、多様化による安全の確保

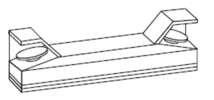
デジタル3重制御系の例



9

安全性の原理 ー ③フール・プルーフ

- ヒューマンエラーの防止
- 間違った操作ができない構造



両手操作制御装置 JIS B 9712:2006

10

安全性の原理 ー ④セーフティ・カルチャ

- 組織エラーの防止
- 組織の安全文化の確立

6S活動
整理、整頓、清掃、清潔、躾
＋
安全（Safety）

中国Harbinのタービン工場

11

安全性の原理

安全性の原理 ー 複雑になるほど高度な安全性原理が必要になる

① フェイル・セーフ（停止安全可）
故障時に安全側に動作する
② フォールト・トレランス（停止安全不可）
多重化、多様化による安全の確保
③ フール・プルーフ（ヒューマンエラー防止）
間違った操作ができない構造
④ セーフティ・カルチャ（組織エラー防止）
組織の安全文化の確立

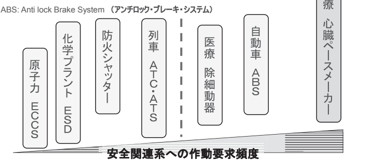
12

安全関連系は利用環境と独立に設計できるか？

13

安全関連系への作動要求頻度

ECCS: Emergency Core Cooling System（非常用炉心冷却装置）
ESD: Emergency Shutdown System（緊急停止装置）
ATC: Automatic Train Control Device（自動列車制御装置）
ATS: Automatic Train Stop Device（自動列車停止装置）
ABS: Anti lock Brake System（アンチロック・ブレーキ・システム）



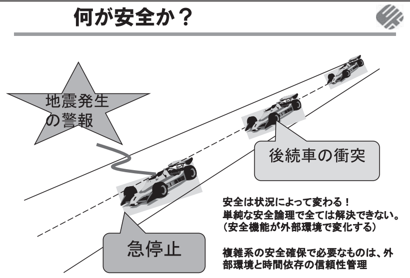
14

作動モードに依存した安全管理

低頻度作動要求モード いざという時に作動	高頻度作動要求又は連続作動モード 常時作動で安全確保
例：防火シャッタ	例：心臓ペースメーカ
停止安全が成立	停止安全が非成立
万一の場合に作動	壊れると直ちに危険になる
普段壊れていても危険な状態には至らない	定期的な作動確認試験ができない
定期的に作動確認をできる	安全装置の多重化などで信頼性を高める必要がある

15

何が安全か？



安全は状況によって変わる！
単純な安全論理で全ては解決できない。
（安全機能が外部環境で変化する）

複雑系の安全確保で必要なものは、外部環境と時間依存の信頼性管理

しかし、現実的には、割り切りが必要

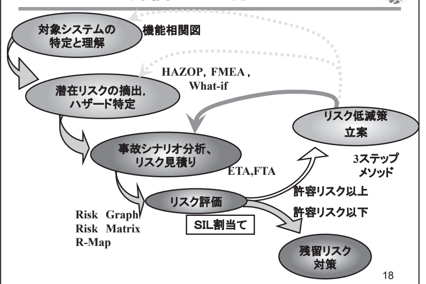
16

どうすれば安全を守れるか？

- 信頼性・安全性・リスクという概念の理解
- リスクをできるだけ少なくする設計
  - ✓ リスク・ゼロのシステム＝動かないシステム
  - ✓ 合理的な範囲でリスクを最小化（ALARP）
- どんな安全設計が可能か
  - ✓ 停止安全が成立するもの（FA機器、ロボットなど）
  - ✓ 停止安全が成立しない複雑な系（原子力プラント、飛行機、列車、車、エレベータ、・・・）
- 規格に基づく設計ー規格にまどわされず原理を理解して設計する

17

リスク評価の進め方



18

主なリスクアセスメント技法

技法	概要
What-if	非体系的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。
FMEA Failure Mode and Effect Analysis	製品および製造プロセスについて故障モードによる影響を分析して製品やプロセスの問題を解決する手法である。製品が使用される段階で起こりうる欠陥や異常な状態などを分析する。
HAZOP Hazard and Operability Study	通常状態からのズレ（設定の温度や濃度）が発生した場合にその原因と発生する結果の事象を特定する。
FTA Fault Tree Analysis	システムの特定故障を想定して、その発生原因を上位レベルから下位レベルまで論理的に展開し、最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める方法である。
ETA Event Tree Analysis	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。
Risk Graph	ツリー形式で示される方法で、想定される危害のひどさ、危険源／危険事象／危険状態にふらされる頻度、回避の可能性などがリスクパラメータとなる。
Risk Matrix	危害の発生頻度と危害のひどさを定性的に見積る手法である。それぞれの要素の分類は4分類する場合や6分類する場合など任意である。
R-Map	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。それにより対象製品を客観的な視点、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）日科技連が推進している。

19

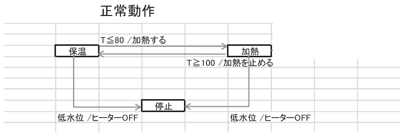
複雑システムのリスクアセスメント

対象システムの機能表現
危険事象のモデルvs正常機能のモデル

FTA,ETA,FMEA
HAZOP
Markov Process Model
Risk Graph
Multi-level Flow Model（MFM）

20

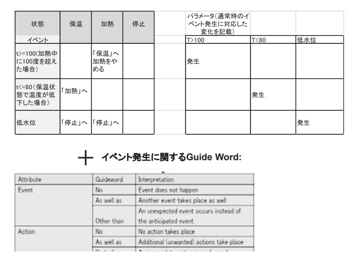
事故シナリオの予測（ポットを事例として）



状態遷移図

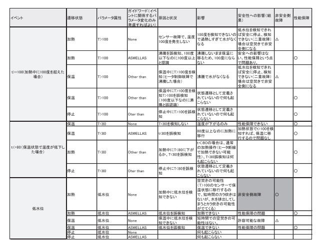
21

状態遷移表（状態遷移図から半自動で作成）



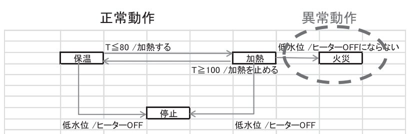
22

状態遷移表に基づくHAZOP（漏れのない事故シナリオの抽出）



23

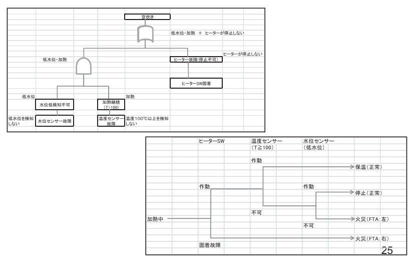
事故シナリオの予測（ポットを事例として）



状態遷移図
（正常動作＋異常動作もモデル化）

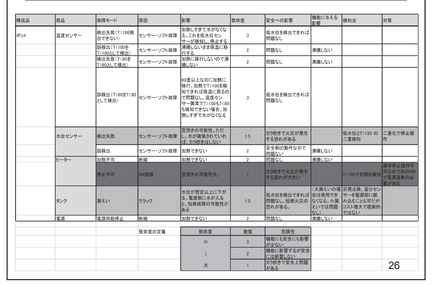
24

FTA&ETA（状態遷移図から手動で作成）



25

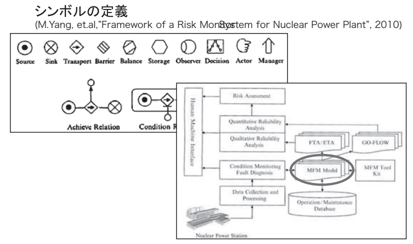
FMEA（状態遷移図から手動で作成）



26

Multi-level Flow Model（MFM）

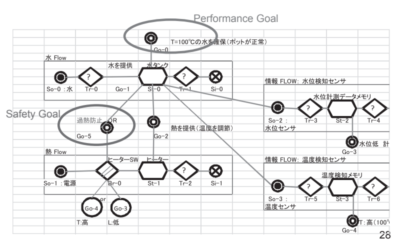
シンボルの定義
(M.Yang, et.al,"Framework of a Risk Monitor System for Nuclear Power Plant", 2010)



27

Multi-level Flow Model (MFM)

（流体、熱、情報の流れを、Part-Whole/Means-Endの多層関係でモデル化）



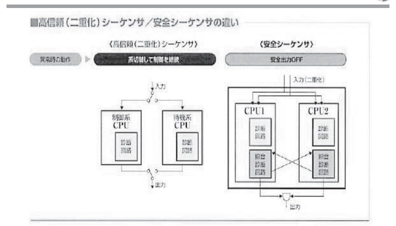
28

安全系の実現例

多重化、多様化にもいろいろな実現法がある

29

三菱電機：安全シーケンサと高信頼性シーケンサ



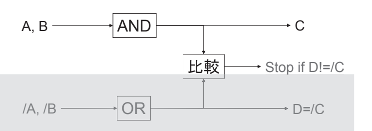
安全シーケンサ：故障を検出することに重点（故障時は安全側で停止）
高信頼性シーケンサ：止めないことに重点
→アーキテクチュア設計が重要

組込みシステム研究会

30

シーメンス：安全PLC
第20回JASA/ETセミナー 2010年6月20日

ソフトウェアによるSIL3レベルの冗長システム
2台のCPU → 1台のCPUで実現



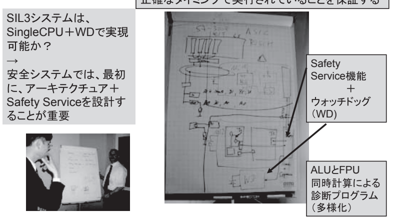
逆の論理を用いた診断プログラムの自動生成
Diversity（多様性）

31

Exida社(ドイツ)訪問

Safety Service機能＝正確なイベントシーケンスが正確なタイミングで実行されていることを保証する

SIL3システムは、SingleCPU＋WDで実現可能か？
→
安全システムでは、最初に、アーキテクチャ＋Safety Serviceを設計することが重要



32

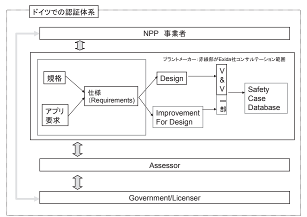
Ⅳ．機能安全の将来動向と教育体系

1. 複雑システムのリスクアセスメントと安全設計
2. 認証のためのツール
3. 機能安全の教育

ドイツの湯たんぽ

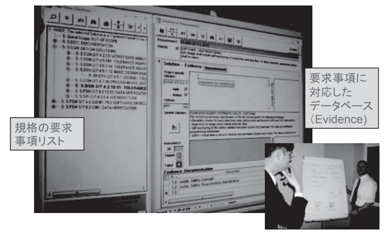
33

ドイツの認証体系（原子力プラントの事例）



34

Exira社のツール ツールの重要さ：Safety Case Database



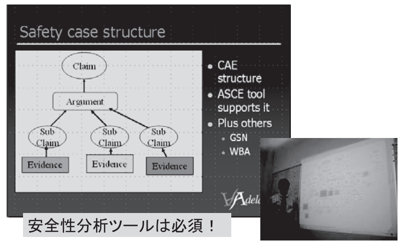
35

Adelard社／City-University-London訪問

- 15人のメンバーによる大学発ベンチャー
- 独立機関としてのV&V
- Safety Caseツール（Claim-Argument-Evidenceによる階層的安全要求事項の整理）

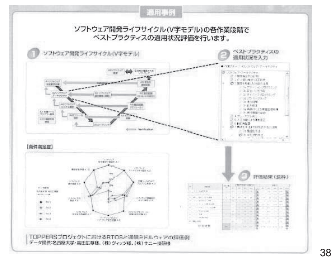
36

Safety Case（Adelard社）



安全性分析ツールは必須！

IEC61508に基づいたソフトウェア安全性評価ツール 安診太郎

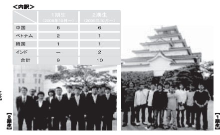


38

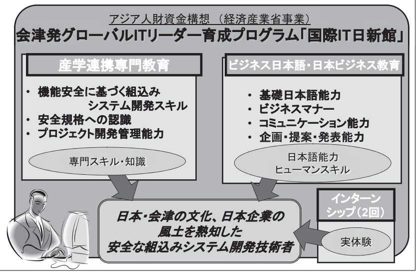
Ⅳ．機能安全の将来動向と教育体系

1. 複雑システムのリスクアセスメントと安全設計
2. 認証のためのツール
3. 機能安全の教育

アジア人財Pj・大学院での講義



会津大学アジア人財プログラムの全体像



専門プログラムの構成と特徴

「安心・安全な組込みシステムの基礎と実践」（第4学期、1.5h×2コマ×8週）
【特徴】・組込みシステムのエッセンス（基本知識）習得
・組込みシステムの安心・安全性
・企業（外部講師）の実践的知識
・素養も教育

「機能安全システムの基礎と実践」（第1学期、1.5h×2コマ×8週）
【特徴】・機能安全の数学的基礎と分析手法の習得
・機能安全の概念と世界標準規格
・企業の実践的機能安全対応の実際（安全評価ツールとRTOS）
・基本能力と素養の教育

「プロジェクトマネジメントの基礎と実践」（第3学期、1.5h×2コマ×8週）
【特徴】・プロジェクトマネジメントの基礎（動向と知識体系）
・プロジェクトマネジメントの技術
・プロジェクトマネジメントの実際（パッケージ型開発、オフショア開発、国家プロジェクト）

教材開発（機能安全の理解）

- 安全失敗事例・デジタル系の故障の概念
  - ソフト・ハードを含めた工学システムの安全系の大事さを失敗事例から学ぶ
- リスクアセスメントと機能安全
  - 工学システムのリスク分析法、機能安全でのリスク制御法
- システム工学・信頼性解析
  - 信頼性評価、HAZOP、FMEA、FTAなどの安全性評価法
- 機能安全の基本的考え方
  - IEC61508の基本的考え方とPart-1～3の具体的説明
- 機能安全のための診断技法や開発プロセス
  - CPU・メモリの診断技術、ハードウェア故障と診断に関する知識、ネットワーク診断技法、ソフトウェア開発プロセスなど
- 機能安全対応システムの実際
  - 安全のデバイス（IEC61508認証安全シーケンサなど）の開発事例
  - 機能安全対応のネットワーク構築事例
  - 安全RTOSの考え方と事例、安全アプリケーションシステムの構築事例
- ソフトウェア開発ツール
  - 各種の開発ツールの具体例、半形式手法、形式手法などのソフトウェア開発手法、コーディング規約等についての教材

42

「機能安全システムの基礎と実践」 内容と実施状況
～基礎知識 ・理論～

	Week1. 4/09	Week2. 4/16	Week3. 4/23	Week4. 4/30	Week5. 5/07	Week6. 5/14	Week7. 5/28	Week8. 6//4
目的	事故例と機能安全の必要性 機能安全規格の概要	リスクアセスメントの全体像	リスク分析 などの基礎知識	ハードウェアの機能安全	ソフトウェアの機能安全	機能安全システムの開発プロセス	機能安全RTOS	機能安全の応用技術
概要	事故例 機能安全（FS）とは IEC61508（1） リスクモデル ALARP 安全度水準（SIL）の決め方 Life Cycle 世界の動向	リスクアセスメントと機能安全	信頼性解析および故障検出技法	IEC61508（2） 潜在危険分析と安全度水準	IEC61508（3） ソフトウエア開発手法 ソフトウエア検証手法 ソフトウエア構成法	V モデル V & V Safety Case Base開発 認証プロセス	機能安全対応RTOSへの要求 アーキテクチャ 時間保護 メモリ保護 割込み等 各種安全RTOSの比較	FSNet FSDevice FSAppli. FS教育
担当講師	程教授	兼本教授	兼本教授 ガイア 川原 氏	兼本教授 ガイア 川原 氏	宮崎教授	荊雷講師 程教授	程教授 荊雷講師	荊雷講師 程教授

43

「機能安全システムの基礎と実践」 内容と実施状況
～企業取組（外部講師）、演習、発表～

	Week1. 4/09	Week2 演習 4/16	Week3. 4/23	Week4. 調査結果の発表会 4/30	Week5. 5/07	Week6. 5/14	Week7. 演習 5/28	Week8. 学習成果発表会と総括 6/4
目的	機能安全の世界動向と日本の取り組みの把握	機能安全システムの設計ツールの理解	企業・社会からみた機能安全システムへの要求	国際視野から自国の商品安全性の現実と対策	機能安全系開発に必要な知識・スキル・素質	現場の経験と取り組みの紹介	機能安全OSの活用法の学習	学習成果の発表 総括
概要	日本の機能安全への取り組みについて～ 信頼性、安全性から機能安全	機能安全のツール設計～「安診太郎」の概要と利用法の演習	日本の機能安全ソフトウェア開発の現状と技術動向 ～事例：自動車に於ける機能安全ソフト	諸国の留学生が自国の製品品質や事故例を調査し、発表・議論する	機能安全な組込みシステムのエッセンスを多角的な視点から教えてもらう	現場からみたソフトの機能安全システム～ ソフトウェアの機能安全の安全度水準について	機能安全OSを利用するプログラミングAPIの例、「Integrity」安全度水準別API利用法と演習	私が見た機能安全な組込みシステム 総括：皆の経験の交流
担当講師	情報処理推進機構 門田氏	東芝システムテクノロジー 平山氏	ヴィッツ 服部氏	内外の先生 コンソーシアム企業	日本機能安全 吉岡氏	ビジネスキューブ・アンド・パートナーズ 藤原氏	アドバンスドデータコントロールズ 慶野氏 福冨氏	内外の先生 コンソーシアム企業

44

安診太郎の使用実績例

■会津大学では「機能安全システムの基礎と実践」教育で使用し、効果を上げることができた。

出展
会津大学HP：
fukushima.jp/asia/trissinkan/report2

45

トピックス

講義スライドから

46

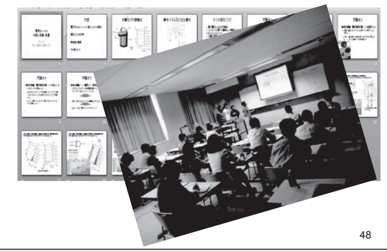
成果発表会から（電気ポットのリスク分析） トピックス

- 学んだ知識をフル活用してのグループ検討＆発表
- 課題
「機能安全手法に基づいた電子ポットのリスク分析と機能改善の提案」
- インプット：電気ポット仕様書（※）

※出典：特定非営利法人組込みソフトウェア管理者・技術者育成研究会

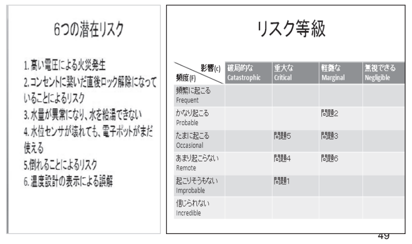
47

グループ2の検討結果は？ トピックス



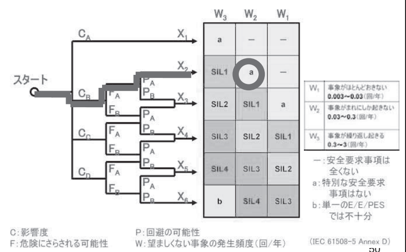
48

潜在リスクの洗い出しとリスク等級 トピックス



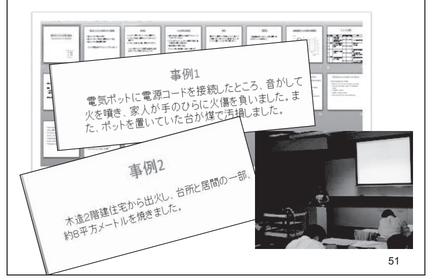
49

電気ポットのSILの評価 トピックス



50

グループ4の検討結果は？ トピックス



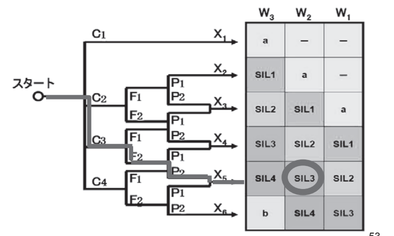
51

リスク判定 トピックス

パラメータ		クラス	
影響度（平均的な死傷者数）	C1	軽症	
	C2	0.01～0.1	
	C3	0.1～1.0	
	C4	1.0以上	
平均曝露確率F	F1	人がまれか比較的そこにいる確率（0.1以下）	
	F2	人が頻繁か常にいる場合（＞0.1）	
平均回避失敗確率P	P1	回避が可能（0.1以下）	
	P2	回避が困難（＞0.1）	
危険事象の起こり易さ（平均）W	W1	事象がほとんどおきない 0.003～0.03（回/年）	−1.5＞logW1≧−2.5
	W2	事象がまれにしか起きない 0.03～0.3（回/年）	−0.5＞logW2≧−1.5
	W3	事象が繰り返し起きる 0.3～3（回/年）	0.5＞logW3≧−0.5

52

SILの評価 トピックス



53

最後に

- 複雑システムのリスクアセスメントと安全設計
  - 多様なリスク分析法の採用、統合化
  - 多様な安全関連系の実現
- 認証のためのツール
  - 安全の可視化＝説明責任
- 機能安全の教育
  - 基本原理の理解と実務知識

54

ご清聴有難うございました。

JASA
安全性向上委員会
製品安全WG

お問合せ先 ：
社団法人組込みシステム技術協会
東京都中央区日本橋浜町1-8-2
TEL：03-5821-7973 FAX：03-5821-0444
E-mail：jasainfo@jasa.or.jp
http://www.jasa.or.jp/

55

平成22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23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