VSE+SS 合同研究会成果レポート

情報サービス産業協会 VSE（基本開発プロセス）研究会 / VSE+SS 合同研究会

ここに報告する研究会成果レポートは 2016 年 1 月に作成したもので、本文に続き、2 つの解説と 1 つのプロセス定義文書で構成されています。

安全・安心なソフトウェアのための基本プロセスガイド

VSE+SS 合同研究会一同

1　このレポートの目的

ソフトウェア／システム開発に関して、比較的に小規模な開発組織の開発プロセスの標準が、国際規格（VSE 規格、ISO/IEC 29110[1] シリーズ）として定められています。その規格の基本は、クリティカルでないソフトウェアの開発を想定しています。一方、現代社会では、どのような開発でもセキュリティが課題となり、また特に組込み系開発では安全性（セーフティ）が幅広く課題となっています。VSE+SS 合同研究会[2] では、そのような課題に対応するために、VSE 規格の拡張として、セキュリティの要素とセーフティの要素を付加した開発の手引きを産業界に提案することとしました。

本レポートでは、VSE+SS 合同研究会の討議経過を簡潔に述べ、その中で開発されたプロセスガイドと、そのプロセスガイドと一体となって提示されるべき「実施指針」（「セーフティの基礎」／「システム開発の情報セキュリティの基礎」）の意義を解説します。そして、それら「ガイド」／「実施指針」の活用により、小規模なソフトウェア／システム開発組織での成果物のセキュリティ／セーフティ品質の向上を図ることを提案します。

2　VSE プロセスとセキュリティ／セーフティプロセス

実は、セーフティにかかわるプロセスの標準は、国際規格として ISO/IEC 15504-10[3] が数年前から提供されています。また、国際的な討議や検討において、セーフティとセキュリティは、それらに取り組むプロセスの面で見るとあまり違わないといわれてきています。

それらの動向を踏まえて、また合同研究会内で提案された二、三の案を踏まえて、ISO/IEC 15504-10 の内容をセキュリティが含まれるものに拡張するのが妥当だろうという結論となりました。この ISO/IEC 15504-10 は、一般的なプロセス標準があることを前提として、それにセーフティについてのプロセスを追加するものです。そこにさらにセキュリティの要素を付加しようとしている。また、小規模開発組織（VSE）向けに、プロセス定義を少しコンパクトにすることを行います。

ところで、一般的なプロセスの標準化は、これも国際規格では略称で SLCP[4] と言われるもの（詳しくは、ISO/IEC 12207 と ISO/IEC 15288）があります。これらにセーフティを加えるのが、元となった ISO/IEC 15504-10 規格の立場です。

1　ISO/IEC 29110-2（JIS X 0165-2：2013）等。なお、本研究会のレポートは、特定領域への VSE 規格の拡張適用方法を定めた ISO/IEC 29110-2-2：2016（発行準備中）を参考にしたものです。

2　VSE+SS 合同研究会は、（一社）情報サービス産業協会 VSE 普及部会、（一社）組込みシステム技術協会安全性向上委員会の各有志メンバー、一般産業界の組込み系開発に関わる有志メンバー、そして本文に述べた課題に興味のあるその他の有志メンバーで構成された合同の研究会です。2014 年ころから 2015 年まで活動を行いました。

3　ISO/IEC 15504-10：2011　Process assessment — Part 10：Safety extension

4　ISO/IEC 12207：2008 Software life cycle processes（JIS X 0160：2012 ソフトウェアライフサイクルプロセス）、ISO/IEC/IEEE 15288：2015 System life cycle processes（JIS X 0170：2013 システムライフサイクルプロセス）

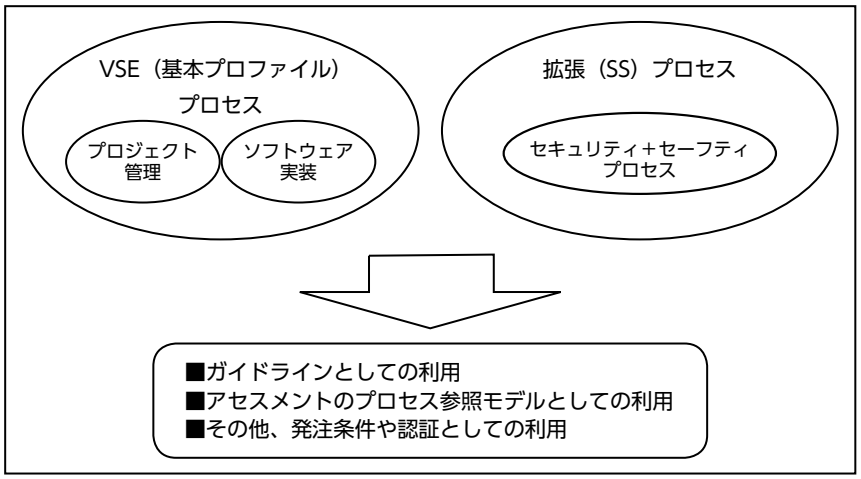


図１　VSE+SS のプロセスガイド（セキュリティ＋セーフティを SS と略す）

しかし、VSE + SS 合同研究会は、小規模開発組織向けでコンパクトな基本開発プロセス標準である VSE 規格を出発点としています。そのため、ここに提示する VSE+SS プロセスガイドでは、「VSE 規格のプロセス」+「セーフティとセキュリティのプロセス」を小規模開発組織に必要なプロセスとしています。一般的にクリティカルな要素がない開発ではセーフティとセキュリティの部分は不要かもしれませんが、現在の多くの開発では（それも日本での産業・ビジネス目的・公共目的の開発では）セーフティとセキュリティの要素が重要になると考えています。

図１に示すように、基本プロセスやセキュリティ／セーフティプロセスはプロセスアセスメントにおけるプロセス参照モデルとして利用することができます。このための利用法の詳細は、ISO/IEC 15504 のプロセスアセスメント（俗称 SPICE アセスメント）として知られています。またそのアセスメントサービスを提供するビジネスも存在しますので、それらの情報／サービスをご利用いただければと思います。

詳しく言えば、プロセスアセスメントのためには、プロセス参照モデル（PRM という）に加えて、より詳細なプロセスアセスメントモデル（PAM という）を開発して適用する必要があります。しかし、この合同研究会の成果として PAM は提供していません。

VSE のプロセスと SS プロセス（セキュリティ＋セーフティプロセスの略記）は少し雰囲気が違います。VSE のプロセスは基本開発プロセスでありソフトウェア／システムのライフサイクルの流れに対応しています。SS のプロセスはそれと並行して実施されるものです。必要なら SS プロセスで述べられていることを VSE のプロセスの中に組み込んで利用してもよいでしょう。

合同研究会の成果物の利用法としては、アセスメントの実施による第三者的な評価を実施するまでもない場合は、開発組織が自身のプロセスを明確にする場合のガイドラインとして利用することができます。さらに、IT システムの発注者が VSE 組織に対して発注条件を設定する場合の手引きとして利用することも有効でしょう。もっと進んで、アセスメントの結果をプロセスの認証の形式で確実にするケースも想定できます。

3　セキュリティ／セーフティの「実施指針」

VSE+SS 合同研究会では、多くの活動をセキュリティとセーフティに関する各「実施指針」の作成にあてました。その理由を説明します。

一般にソフトウェア／システム開発のプロセスのモデル適用やアセスメントの実施では、現場の人々においてプロセスモデル定式化の背景的なことやプロセス実施で実務的にはどのような事柄に注意すべきかがあまり理解されずに、形式的な面のみが前面に出てしまうと反省されることがよく

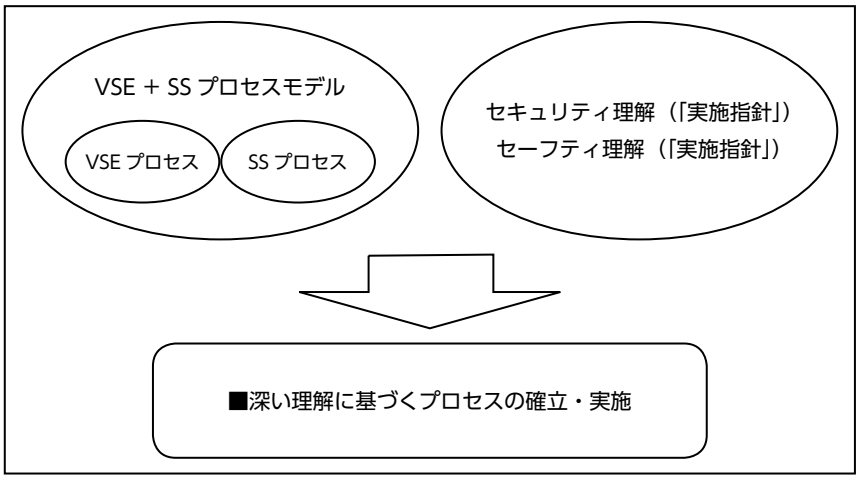


図２　実施指針の活用

あります。セキュリティとセーフティについては、特にこのような幅広い理解の重視や、その理解促進のための現場マインドの醸成が重要です。

そのような事情から、VSE+SS 合同研究会では、そもそもなぜセキュリティとセーフティに取り組むのか、どのようなスタンスとマインドで取り組むべきなのかを示す「実施指針」を前提条件として開発することとしました。この「実施指針」に類似する内容の概説書は世間に多くありますが、今回の「実施指針」は、ソフトウェア／システムの開発プロセス実施に際して、そのための前提的な理解を求めて簡潔な基本知識をまとめ、2 章に述べたような VSE+SS プロセス実施を確実にするための資料としたことに意義があります。

この「実施指針」の具体的な利用法としては、VSE に当たる開発組織が自身のプロセスを強固なものにするための共通基礎理解として活用したり、ソフトウェア／システムの発注側が受注・開発側に対して必要な基礎知識・スキルとして内容理解を求める材料として活用したりすることなどが想定されます。（図 2 を参照。）

4　他の規格や基準との関係

プロセスの基準には、VSE 規格の他に上でも触れた SLCP や日本国内での「共通フレーム」[5]、IPA 作成の ESPR[6] などもあります。VSE+SS 合同研究会で開発した考え方の枠組みは、プロセスモデルとして VSE プロセスモデルでなくこれらのプロセスモデルを利用することを妨げるものではありません。しかし、多くの小規模開発組織にとっては、VSE プロセスモデルの適用が便利でしょう。

セーフティに関しては、たとえば自動車分野での ISO 26262 規格のように、多少厳しい基準適用スキームを持っているケースもあります。そのような場合に発注元が示すセーフティ関連要求事項は厳密に満たさなければいけませんが、それらを実施する際の背景やセーフティマインドの醸成には VSE+SS 合同研究会の成果物が役に立つと思います。

セキュリティに関しては、セキュリティの「実施指針」にも述べられているように、2 つの観点（テーマ）を区別する必要があります。VSE 組織にとってのセキュリティに関するテーマは、(1) 組織が企業活動上で管理する情報資産に関わるセ

5 （独）情報処理推進機構編・発行「共通フレーム 2013」、2013 年、（https://www.ipa.go.jp/sec/publish/tn12-006.html を参照）
6 （独）情報処理推進機構編【改訂版】組込みソフトウェア向け開発プロセスガイド」、翔泳社刊、2007 年（http://www.ipa.go.jp/sec/publish/tn07-005.html を参照）

キュリテイ（ISMS 規格等が典型的に扱う）のテーマと、(2) 組織が開発・提供する製品が実現すべきセキュリティ品質のテーマとの、2 つのテーマとがあるということです。VSE+SS 合同研究会の成果物は基本的には (2) の観点に沿ったものです。これにあたる国際規格としてはコモンクライテリア[7] というものもあります。

5 成果物活用をどう使うのか

VSE+SS 合同研究会の成果物は、軽量な扱いやすいものですから、それぞれの開発現場で、それぞれのニーズに合わせて必要なカスタマイズをし、本来の必要な業務高度化の成果に結び付けていただくのがよいと思います。このテーマは（実は）国際的にも先進的な取組みですから、皆さんの組織が競争力をつけ、マーケットで通用する確実な実力を身に着け、ビジネス上の信用力を向上させることに役立てていただければと思います。

その他の具体的な使い方の例としては、JISA から出版された「VSE 標準導入の手引き」[8] に記載されている「VSE 標準活用事例」が参考になるでしょう。

■ VSE+SS 合同研究会メンバー

座長	伏見　諭	東海大学
	足立久美	
	倉持俊之	TIS 株式会社
	塩谷和範	
	菅原博之	ソニー株式会社
	田渕一成	ビジネスキューブ・アンド・パートナーズ株式会社
	那須　誠	一般社団法人　組込みシステム技術協会
	錦見美貴子	国立研究開発法人　産業技術総合研究所
	堀　武司	地方独立行政法人　北海道立総合研究機構
	三輪一義	一般社団法人　組込みシステム技術協会
オブザーバ	山下博之	独立行政法人情報処理推進機構
事務局	尾股達也	一般社団法人　情報サービス産業協会
事務局	佐藤厚夫	一般社団法人　情報サービス産業協会

7 ISO/IEC 15408:2009（Security techniques-Evaluation criteria for IT security; Common Criteria とも略称）（JIS X 5070：2011 セキュリティ技術ー情報技術セキュリティの評価基準）（http://www.ipa.go.jp/security/jisec/cc/　をも参照）

8 （一社）情報サービス産業協会編「VSE 標準導入の手引き」㈱アイエージー刊、2014 年

[解説]

システム開発の情報セキュリティの基礎 ～小規模開発組織のセキュアな開発にむけて～

伏見 諭、那須 誠、三輪 一義
VSE+SS 合同研究会一同

要 旨

ITやネットワークの発展に並行して、そのセキュリティ面の課題が指摘され、また実際のセキュリティ上の攻撃が日常的に行われるようになって久しい。

しかし、ソフトウェアを組み込んだシステムを開発する際に、そのようなセキュリティへの対応を高い信頼性で実施するにはどうすればよいかは、あまり明確になっているとは言えない。本稿は、特にソフトウェア開発を行う小規模組織のマネージャ層やエンジニアが、実際の業務においてどのようにセキュリティの課題に対応すべきかの基礎的知見を提供することを目的とする。いわゆる組込み系システムに焦点をあてている。

1 システム開発の情報セキュリティとは

1.1 情報セキュリティの２つの課題

いま（特に組込み系等の）ソフトウェアを中心とするシステム開発で、セキュリティを問題にする場合に、開発組織の（持つ、または取扱う）機密情報の漏えい防止などを主な着眼点とした取組みと、開発対象であるシステムをセキュリティ的に強固なものとしなければならないという取組みの２つの課題がある（表1）。両者ともに重要なものだが、本稿では、後者の視点を中心に基本的な着眼点と開発活動の指針を提供する。

組織の情報資産を守るセキュリティ	情報漏えいなどから組織活動を守る。 情報の保全とサービス継続の活動。
製品・システムのセキュリティ	機密性、インテグリティ（後述：２章参照）など製品・システムとサービスの全体的なセキュリティ上の能力を確保する。

表１　開発における情報セキュリティの２つの課題

製品等のセキュリティを問題とする上でも、技術面の課題と管理面の課題がある。これについては４章以下で説明する。

1.2 セキュリティ確保の責任の所在

システムの開発においては、開発チームの他に、発注者や社内の他部署が関係者（ステークホルダ）となることが多い。開発されたシステムのセキュリティが確実となるためには、正しい運用設定が必要だが、システム／サービスの運用者・利用者が、利用時のシステムのセキュリティ設定等に関与することも多い。

それらの多くの関係の中で、どのようにシステム全体としてのセキュリティを確保していくか、適切に責任分担がなされ、対策がとられる必要がある。このことはシステムにセキュリティホールを作らないという意味で非常に重要である。システム開発の２者間取引では、そうした責任分担が契約的文書の中に明確に記載されていることも重要となる。その際、発注者がセキュリティ課題を

分析（・設計）し、受注者がそれを実装するケースや、逆に受注側のソフトウェア開発者が専門家としての知識・スキルとノウハウに基づき、セキュリティを自己の責任で確保するケースなど、さまざまである。受発注者の間で責任分担を明確にし、かつ円滑なコミュニケーションを保つことがセキュリティ確保の基礎となる。

本稿は、開発に携わる様々な立場の方が、情報セキュリティについて共通に理解すべき課題と、それぞれの立場で責任を持つべき課題と対応方法等について、以下に詳述する。2章では製品開発の情報セキュリティの概要を説明し、3章ではセキュリティ対策の実際の展開の仕方について技術面を中心に説明し、4章では管理的な側面での課題を説明する。5章では、基本的な当時者である発注側と開発ベンダ側との役割分担について説明し、6章では過去事例からの教訓について紹介する。

2　情報セキュリティの基本

情報セキュリティは、現代社会の抱える出口のない大きな問題とも言えるが、多くのセキュリティのニュースに接して、漠然と「セキュリティの脅威に対抗しなければいけない」と言っていても場当たり的になるだけである。そのような対応では、対処すべき課題は膨大となり思考が拡散し、結果的には「大変だからまともには取り組めない、そこそこで我慢しよう」ということになる。その結果生み出されてしまったセキュリティの弱点を突かれることになりかねない。

開発対象システム／製品における情報セキュリティ上の課題を整理し、危険性を理解した上で、自分自身を含む開発者・関係者の知識リソース、スキルリソースを整理して活用しかつ、開発者及び関係者の円滑なコミュニケーションを図りながら開発することが重要である。

2.1　セキュリティリスクとは

セキュリティ対策は、ある種のリスクマネジメントとしてとらえられる。ここでのリスクは攻撃を仕掛けてくる脅威源、攻撃を許してしまう防御の脆弱性、攻撃の結果がどのように製品（また、それを含むシステム）に関わる情報資産、および、製品の利用者や関係者の情報資産にどう影響するかの3要素に分解してとらえられる（図1）。この「脅威」、「脆弱性」、「影響」の分析が、リスク分析の3要素である。

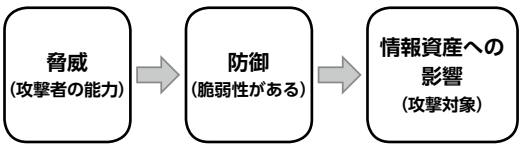


図1　攻撃、防御（脆弱性）と影響

脅威・脆弱性・影響というリスクの3要素とともに、機密性・インテグリティ・可用性・真正性（認証性）というセキュリティが守るものの種別を組み合わせて、セキュリティの具体的な課題を詳細にとらえていくことができる。セキュリティ課題がとらえられると、それに基づいて、セキュリティ対応策を考えていくこととなる。

これらの、機密性、インテグリティ、可用性、真正性（認証性）のそれぞれの意味を表2に示す[1]。

セキュリティの守るもの	説　明
機密性	秘密にすべき情報／サービスが秘密に保たれていること。
インテグリティ	利用対象の情報／サービスの情報内容が正しく保たれ提供されていること。
可用性	必要な時に妨害されずに情報／サービスを利用できること。
真正性（認証性）	不正な人やサイト、プログラムなどではなく、正当な主体（人、もの、プロセス）であることを保証できること。

表2　セキュリティの目的

1　これらの用語の詳細について、たとえば参考資料 1)、2) などを参照。

セキュリティで守るものとしては、これらに加えてプライバシーの課題、否認防止[2]の課題、アカウンタビリティ（責任追跡性）の課題などを加えることがあり、製品面のセキュリティの達成のためにそれらを意識すべき場合がある。

一般的なリスク対応には、(a)リスクを「緩和」する方策のほかに、(b)リスクの関係するおおもとの施策そのものをやめてしまう「回避」、(c)リスクの負担を第三者に肩代わりしてもらう方策をとる「転嫁」、また(d)緩和が一定程度進んだがある程度のリスクが残り、その残存リスクをやむを得ないとしてしまう「受容」、という方策もあるが、通常は「緩和」する方策が探られる。

2.2 セキュリティリスクの重大特徴と防御

情報セキュリティにおけるリスクには、悪意を持った攻撃者が不断にシステムの欠陥と防御の穴を探し出し攻撃を加えるという特異性がある。攻撃はアットランダムに行われるのではなく、攻撃者のスキルと知識がだんだんに蓄積され高度化するという特異性もある。そのため、いったん攻撃方法が確立され、かつ、執拗に狙われると、その攻撃はほぼ確実に成功するものとみなさなければならなくなる。逆に言えば、それまでの防御策は無効化する。例として、一時無線LANではWEPという方式が広くおこなわれたが、WEPの脆弱性が発見されその脆弱性をつくツールが流布するようになると、WEP方式自体が無効なものとみなさなければならなくなった。

このような攻撃を単一の防御策で完全に封ずることは不可能に近い。そのため連続した防御壁によるリスク管理手法である「多層防御」が有効である。下の図2はいわゆるスイスチーズモデルと呼ばれる多層防御のイメージを表すものであるが、複数の防御方策を設け、一つの防御が突破されても、次の防御層で阻止するという考え方である。仮に、一旦不正な攻撃による内部侵入を許したとしても、システムの暴走を起こす攻撃は許さず、場合により代替システムに切り替える、また外部への不正な情報流出は許さないといったような第二、第三の防御策を考えておくことが重要である。

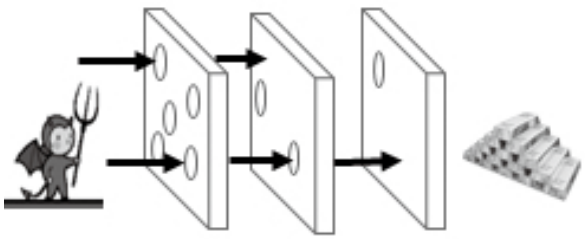


図2　多層防御のイメージ

2.3 リスクアセスメント

セキュリティリスクに対応するためには、情報資産、脅威と脆弱性、攻撃を受ける場所・時間などの対策すべき要素を、重要な情報資産とシステムの特性の把握や過去の事故事例などに基づいて適切にリスク評価し、対策方法を決める必要がある。

開発システムの中には、システム脆弱性があっても、攻撃者の攻撃意図がまったく無いという想定が正しい場合もあり、セキュリティがほとんど問題にならないケースもある（リスクを「受容」する場合など）。どのようなプロジェクトの条件でも同様に厳重なセキュリティ対応が必要なわけではない。

実際のセキュリティ対策については、次章以降で述べる。

2.4 さまざまなケースでのリスクの特色と対策

製品やシステムのセキュリティ対策と一口に言ってもそれらがどのような場でどのような使われ方をするのか、また守るべき情報資産が何なのかによりとるべき対策は多種多様である。以下に実例を述べる。

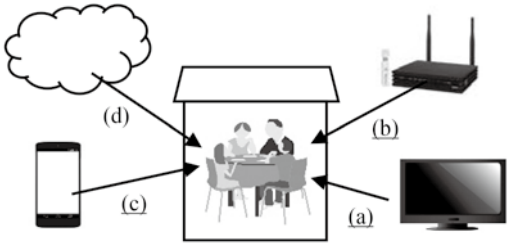
[2] 情報主体が実際には行った行為を行っていないように主張することを否認と言い、インターネット上で行われるコミュニケーションを確実にするには否認の防止が必要となる。

1）ルータ等のネットワーク機器の場合

小規模事業所や家庭などで設置されるネットワークを構成する機器は組込みソフトウェアシステムであることが多く、これに対するセキュリティ対策は企業情報システムのセキュリティ対策と違い、出荷後修正が難しい大量生産機器であり、かつ利用者が専門家でないことが多いことからセキュリティ対策をより綿密に行うことが必要である。これらネットワーク機器は、その機能仕様として、ネットワーク機能とセキュリティ機能をもっていることが多い。そうした機能自体がしっかりしている必要がある。また、機器のパラメータ設定用画面機能など支援的機能や、バイパスを許さない、物理的攻撃で情報を盗まれないといった統合システムとしてのセキュリティもよく検討し対策しなければならない。

2）スマホアプリや情報家電等の場合

情報家電、スマートフォンやNAVIシステムに代表される、ネットワークに接続して日常生活で使う情報機器に組み込むシステムのセキュリティ対策もある。デジタルテレビなどデジタル化、双方向化が進んでおりており、ホームネットワークにつながるデジタル家電がトレンドとなっているが、それらはオンラインでセキュリティアップデートをかけられることが多い。セキュリティアップデートをどのように安全・有効に行うかもセキュリティ課題の一つとなる。図3は情報家電における脅威の例を示すものであるが、このように多様なリスクに幅広く対処しなければならないという特徴もある。



(a) 偽の修正ソフトダウンロード
(b) 問題のあるネットワーク機器
(c) スマホや無線機器からの不正アクセス
(d) 不正サイトへの安易な接続

図3　情報家電の脅威と脆弱性の例

3）業務システムの場合

組込みシステムではないが、企業内で使われる情報システム、ネット通販のシステム、官公庁／団体／一般企業などを紹介するホームページなどの場で使われる製品を考えた場合、それぞれに、守るべき多くの情報資産の多様な特色やセキュリティの要請程度があり、それを明確にし、その結果に照らしたセキュリティ対策が必須となるという課題がある。

3　セキュリティ対応の実際

3.1　セキュリティ機能の要件定義と実装のプロセス

システムを開発する際には、開発している製品の機密性、インテグリティ、可用性、真正性に関わる防御能力等がどの程度であるか、さらに具体的にどの程度の攻撃に耐えられるかが問題となる。これらの能力は、システムのセキュリティ機能要件という形でまとめられることもあるが、セキュア・プログラミングの技術のように、現場の技術能力が製品のセキュリティ品質達成の大きな要因となるようなものもある。本節では、そのセキュリティ品質達成の具体的なやり方を説明する。

1）守るべき情報資産の特定

まず守るべき情報資産を特定する必要がある。ここで、守るべき情報資産とは、製品・システムの使用者と使用状況とに関わる情報、技術的な機密性のある情報、さらに製品・システムが提供する情報サービスのことである。

例：テレビ、エアコン、車などの稼働状況から利用者の行動様式が分かることをプライバシー上の問題とする場合、その「利用者の行動様式デー

タ」が対象となる守るべき情報資産である。

2）リスクアセスメント

リスクの評価・見積りと対策を行う一連の工程をリスクアセスメントと呼ぶ。アセスメントのステップはセキュリティにおいても他の分野のリスク分析と同様である。すなわち；

⑴　守るべき資産の洗い出し
⑵　ハザード（脅威）や攻撃者能力の洗い出し
⑶　システムの脆弱性の把握や評価
⑷　リスクの識別と分析
⑸　上記で特定したリスクの程度の評価と対応策選択の方向性設定

というステップとなる。

このアセスメントに抜けや欠点があった場合、その後の工程で行う対策が不十分になるので、ここでは特に十分に吟味して行わなければならない。

リスクアセスメントは時間・コストの許す限り徹底して行う必要があり、できる限り詳細リスク分析（巻末資料１参照）を行うことが望ましい。

評価の結果によりリスク緩和策が必要となった場合、複数の緩和ソリューションを検討し、有効性とコストパフォーマンスの両面を考慮して選択する。この選択に当たっては、試行を行って効果を見定めるとか、セキュリティツールベンダの示す効果表示値を検討するなどして慎重に行うとよい。

このようなリスクの程度の計算、ソリューション選択にあたっては、できるだけ厳密にという方針で数値的に行う場合もあれば、概要を把握することが重要だという方針で定性的に評価することもあり、それぞれに各種の手法が開発されている（これも巻末参考資料１を参照）。

3）セキュリティ対策のコスト見積もり

上述したように、実際にセキュリティ対策をとるためにはそのための費用（設備・ソフトウェアライブラリ・技術・要員などを含む）と時間の手当が必要である。

また、開発と運用の両方の要員の教育・訓練と、組織としてのセキュリティノウハウの向上を図ることが重要になる。セキュリティ事件・事故が発生した時の、いざというときの費用と対処時間の見積もできる体制が必要になる。

顧客の要求に基づいてシステム開発を行う場合には、特に、顧客にコストについての理解を求めることが重要となる。

4）セキュリティの確実な開発ライフサイクルへの展開

対策方法のセキュリティ機能要件を明確にすることとともに、その目的とするセキュリティを実現する技術としては、たとえば実装段階でセキュア・コーディング等が必須となる。このような、セキュリティ対応の、具体的な開発プロセスへの展開は、実務上で最も重要である。その方法として、たとえば、VSE 規格（小規模組織向けプロセス規格）を参考にし、その基本となる開発プロセスの中にセキュリティ対応事項を織り込むことが考えられる。そのイメージ例については、図４を参照。

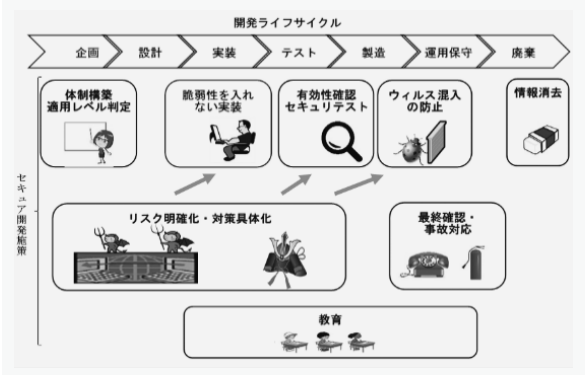


図４　セキュリティを考慮した開発プロセスのイメージ

5）運用時のインシデント対応のプロセス・態勢

セキュリティに関しては、多くの製品が出荷後に問題が見出されたり、新しい攻撃にさらされたりすることが多い。システムの運用設定がまずいためにセキュリティの脆弱性が生じることもある。また、利用した汎用部品のセキュリティホールが発見されることもある。こうした事態に迅速

にかつ柔軟に対処できるプロセス・態勢の構築や、利用者への指導、また、メンテナンス性の考慮等の製品のアーキテクチャ上の工夫も必要である。

6）参考となる情報の活用

上記のような対応を確実に行うためには、信頼できる基準やガイドを参考にするのがよい。それには、例えば、次のようなものがある。

- IPA のセキュア・プログラミング講座等の情報
  https://www.ipa.go.jp/security/awareness/vendor/programmingv2/
- IPA の各種指針（たとえば ESCR など）
  http://www.ipa.go.jp/sec/reports/20150410.html
- CERT-C、国際規格セキュア・ライブラリなどのセキュア・プログラミング指針
- OWASP、IPA などのセキュアな Web サイト開発のための指針
- それらに対応する組織内／プロジェクト内のセキュア開発ルール／コーディングルールとその確実な実装をチェックする静的解析ツールの活用

3.2 セキュリティプロセスの留意点

1）攻撃方法が日進月歩進化していることへの対応

攻撃者の目的は、単なるイタズラから金銭目当ての詐欺に移り、その上に国家の安全を脅かすまで高度化してきている。

IPA や JPCERT/CC などの国内の Web サイト、国際的な情報源などにアクセスして、情報セキュリティの対策についての情報を常に把握しておくことが重要となる。

2）組織管理・プロジェクト管理上の考慮

人材の教育や文書管理を含め必要なセキュリティ品質が確保できる状態になっているかを実態に即して把握する。個々のプロジェクトの実施においても、必要な場合は、セキュリティ品質上の保証を行うためのプロジェクト管理ができるようにする。

3）対象分野で規制等がある場合は対応する

たとえば医療機器分野では、薬事法（日本）や FDA 規制（米国）等に基づく強制的規制や、多くの業界基準が設けられている。これらの分野では規制等への的確な対応を行う必要がある（資料 5 参考資料[3)]を参照）。

4）ライフサイクル全般を見据える

組込みソフトウェアは組込まれるデジタル機器と一体なので、欠陥が発覚した場合、全品のリコール問題まで発展しかねない。組込みソフトウェアでなくても最近のソフトウェアは、システム運用時のセキュリティ対応が重要である。もはや「ソフトウェアは作って終わり」という時代ではない。セキュリティ上では、製品やそれに付随するデータの廃棄や保全ということも重大な問題となる。それ故、製品のライフサイクル（企画、開発、運用、保守、廃棄）全体を見据えたセキュリティの要件定義やライフサイクルを構成する各プロセスの品質向上が特に重要となる。

3.3 セキュリティとセーフティの関係

特に組込み系のシステムでは、セキュリティとセーフティは深く関係している。セキュリティ攻撃の結果としてセーフティが危うくなるケースが多くある。

大きな事例としては、海外での製鉄所へのセキュリティ面でのマルウェア攻撃が、プラント設備の運用を危うくし、一種のセーフティインシデントを発生させている。また、逆にセーフティが崩れると特に可用性や情報保全などの面でセキュリティに影響する。

セキュリティ攻撃の中でも、インテグリティや可用性に関連する攻撃は、このようにセーフティと直接関連する可能性が大きいため、セキュリティとセーフティの課題は一体のものとして分析したり対策したりする方がよいことが多々ある。

4 開発部門／開発企業での体制づくりと意識向上

4.1 取組みのアプローチ

セキュリティ対策には人的投資が前提となり、また企業の風土作りも重要になる。開発を外部委託する場合であっても自社同様の企業風土・対応があるかを点検せねばならず、いずれにしても相応のコストがかかることを予め考慮しておかなければならない。

企業内での実際の風土作りは次のことを考慮して進めることになる。

1）最適な体制の構築

セキュリティ対策では、セキュリティ対応姿勢の明確化やリソースの確保といったトップダウンの足並みをそろえた組織的な対応と、現場の工夫・ノウハウの集積といったボトムアップの取組みとの両輪により情報セキュリティの管理体制を構築することが重要となる。

2）人材育成とノウハウの蓄積・活用

セキュリティ対策は掛け声だけでは空回りしたり、過剰反応となったりすることがある。セキュリティ知識・スキルを身に付けたスタッフの育成、その知識・スキルのアップデートの仕組み、組織的なノウハウ集積（最新情報収集）と活用のためのノウハウリポジトリ構築や、インターネット上にある有用なセキュリティ情報へのアクセス態勢などが重要となる。

対象分野での規制や、デファクトの基準等の知識も欠かせない。その結果必要であれば、適切な対処を行う。

3）カルチャーとマインド形成

自社が情報セキュリティにどのように取組むかについての共通的なマインド形成と、それに対応した実践上のカルチャー作りを重視しなければならない。また、そうした取組みを外部に対してもホームページなどで公表し、「セキュリティ対応が優れていることを自他ともに認められる」ようにすることはビジネスメリットがあるだろう。

4）ガイドラインや標準との付き合い方

次節で紹介するように、国際／国内のセキュリティガイドラインや制度が多くある。それらの自組織にとっての有効性・必要性を見極め、ガイドや制度の文面に過度にとらわれるのではなく実際にどうあるべきか検討し、またノウハウを蓄積しながら、自組織の実力を高めていくようにするのがよい。

4.2 開発組織（企業）運営上の対策と情報セキュリティ認証制度

当然ながら、開発にあたる組織運営そのものに情報セキュリティの対策がなければせっかくの開発物のノウハウや機密情報が外部に漏洩したり、外部から開発中のソフトウェア製品そのものが改ざんされるなどの攻撃をされたりするおそれがある。

情報セキュリティの第三者認証制度を利用したり、参考にしたりすると、体系的に組織運営上のセキュリティ対応を実施できることがある。情報セキュリティ関連の第三者認証制度には巻末参考資料２に示すものがある。

4.3 セキュリティ対策での勘違い

1）認証取得を自己目的化しない。

認証取得は自社のセキュリティ対策の確実性の証明方法としてビジネス的には重要なことであるが、本来必要なのはセキュリティ対策をきちんと行うことであり、そのためには日常の情報セキュリティについての地道な活動が重要である。有効なセキュリティ日常活動の確立の上に認証取得もありうるという順序を踏み間違えないようにすることが望まれる。

2）ルールでがんじがらめにしない。

セキュリティの各種ガイドラインや認証基準が示す指導項目の理由をよく理解できていないと間違った対策や行き過ぎたルールを作ることになる。

例：開発組織内で「USB メモリを使用することで事件事故が発生するそうなので USB メモリの使用を全面禁止する」といった方策を安易に決めることは、「危険そうだから禁止」という、よくある行過ぎ策の代表例である。USB メモリを使わない場合のビジネスの効率性との比較検討や「強制暗号化 USB メモリを採用する方策の検討」などとのトレードオフを評価した上で決定することが重要である。その結果仮に「USB メモリを使用する」ことになった場合には、実際にどのような技術的・制度的対策をとるかを検討し、詳しく運用方法を決定することになる。

4.4 リスクマネジメントとセキュリティ要求事項理解の知識・スキル作り

クリティカルな製品を開発する企業にとって、その社会的責務を果たすためには、開発にあたって常にリスクの評価とリスクの緩和策が正しいものなのか検証する姿勢を持つこと、即ち、リスク分析、リスクアセスメント、リスクコントロール手段の設計と実装、検証、妥当性確認を行うことが必要である。

こうしたリスクマネジメントは一挙に正解に達するのは難しく、分析・設計・実装・テストといった開発ライフサイクルを通じて、リスク対応自体の品質向上のためのライフサイクルを経ることが通常である。リスク評価とリスク緩和の反復プロセスのライフサイクルの概要イメージを図５に示す。

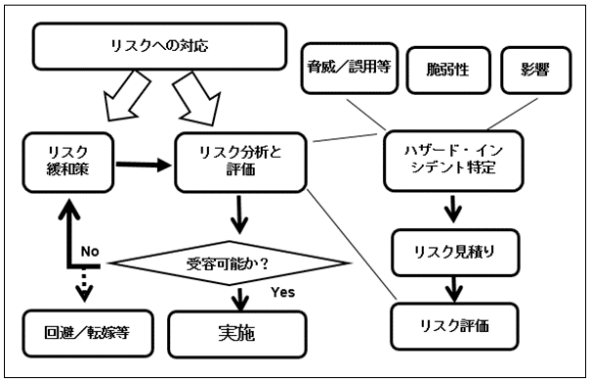


図５　リスク評価とリスク緩和の反復プロセスのイメージ

リスクアセスメント全体を自ら行わず、発注者のセキュリティ要求事項をうけて業務を行っている開発組織の場合は、セキュリティ要求事項の意味や背景を正しく理解する能力、また、必ずしも要求事項に明示されていなくてもプロフェッショナルな業務としてセキュリティ品質確保のために必要なことは何かを理解し実施する知識・スキルが要請される。また、この場合にも、実装・テストの結果を図５の反復プロセスに活かす活動を行う場合がある。

5 発注側と開発ベンダ側のポジショニング

セキュリティの問題の中には、場合により利用者等からの訴訟の対象となったり、報道に取り上げられて企業のブランドを傷つけられたりするものがある。

セキュリティの取扱いについてのそうした面も考慮しながら、よいシステムを開発し、よいサービスを提供するために、受注側・発注側双方の充実したコミュニケーションをベースとして、具体的なセキュリティ課題に取り組む必要がある。

1）発注側メーカは製品仕様に必要なセキュリティ機能を明確にする。
2）受注側開発ベンダは不足しているセキュリティ機能とその開発手法を提案する。
3）受発注側双方の技術を集合した開発プロセスを確立し、それぞれの立場と役割を明確にする。これは開発案件ごとに必要になる。
4）受注側開発ベンダは発注側の仕様を鵜呑みにせず逆提案できるように、日頃から知識・スキルやノウハウを獲得・蓄積する。
昨今では、開発仕様に対してセキュリティ対策が必要な要件を逆提案することが要求されるので受注側開発ベンダは進んで提案できるようになる必要がある。
5）受注者側の基本的スタンスとして大事なことは、要件に含まれているか否かにかかわらず、常にセキュリティを確保することは組織の社会的責務であること、発注者の元々のセキュリティ目標が達成されるべきことを忘れてはならないということである。実装プロセスやテスト等で、自分自身の知識・スキルやノウハウを用いてセキュリティを確保できるようにすることが必要である。

6 過去の事例から学ぶ

セキュリティの取扱いでは、セキュリティに関する利用者の意識等の社会状況の変化や、実際の事故事例に学ぶことが特に重要である。以下に特徴的な事例を列挙するが、それぞれの開発・運用組織でもこうした教訓を技術ノウハウとして蓄積していくことが重要となる。

〈事例 1〉 大規模個人情報漏えい事件

事象：個人情報を含むデータベース運用を外部委託したシステムで、作業員が充電目的と偽り、私用のスマホをシステムのクライアント PC に USB 接続し、個人情報をコピーして業者に販売したとされる事件。

背景：大きくは次の点が指摘されている。

・外部委託した作業員が権限を越えて個人情報のデータベースにアクセスできた。
・システムに USB デバイスが接続されたことを検知する機能が不足又は無効だった。

開発／運用サービスベンダの留意点：

・個人情報データベースなどのアクセス制御を適切に設計・実装するとともに、運用ルールを策定しそのルールに従って厳密に運用しなければならない。いわゆる組織の情報セキュリティにも留意しなければならない。なお、組織の情報セキュリティの詳細については巻末資料 2、ISMS、CMSiS を参照されたい。
・必要・有効な場合、個人情報の暗号化を行ったり USB ポートの使用制限機能を実装したりする。

〈事例 2〉 裁判事例：セキュリティ対策漏れの責任を開発会社が負わされた例

事象：公開 Web サイトにおいて機密情報漏えいが起こり、発注側企業はベンダ側の過失として損害賠償を求めた。2014 年、裁判所は、社会で一般に知られている基準の無視による「重過失」だとして、開発費を超える多額の賠償を求める判決を出した。

背景：

・これまで、開発に伴う責任が問われても、開発費を上限とすることが多かったが、本件では、その契約条項があっても重過失では適用されないという理由で多額の賠償となった。
・IPA が発表している「安全な Web サイトの作り方」という文書等が社会一般に公知の品質基準であるとされた。

開発ベンダの留意点：

・契約書および合意議事録において、双方の責任分担と、仕様の上での「セキュリティ要件の必要／不必要」とについて、できるだけ具体的に記載することが望ましい。

〈事例 3〉 スマホでの情報漏えいにつながる恐れ

事象：スマホでは、多くのアプリが並行動作しており、それらの間で情報の盗み取りが発生する可能性が指摘されている。

背景：

・スマホは、個人情報の宝庫であることから攻撃者のターゲットになりやすい上、使用者の大部分が情報セキュリティに対する意識や知識が少ない一般人である。

・多用される通信経路がハッカーの比較的侵入しやすい Wi-Fi であることや、一見便利な無料アプリにウイルスが仕込まれることがあるなど、さまざまなリスクに晒されている。

開発ベンダの留意点：

・アプリ間情報連携はセキュリティ上の危険性をはらむことをよく理解して、対策・対応が必要であることを強く意識する。

・セキュリティ確保のためにはどのような方策が必要か、プラットフォームベンダ等の提供する情報を漏れなく収集し、適切に対応する。

・「ジェイルブレーク」等、ブラックマーケットで行われている事象とは明確に距離を置き、加担しない。

〈事例 4〉 家庭用テレビのリブート障害

事象：某メーカの家庭向けテレビ受像機が、全国一斉に深夜リブートを繰り返す事象が発生した。

背景：

・テレビのファームウェアは放送電波（特定電波）を利用してアップデートする機能を持つ場合があるが、本件では他社向けを含む特定電波データを、テレビに内蔵されたソフトが上手く取り込めなかったことが原因とされた

開発ベンダの留意点：

・この例のようにネットワーク接続機器などのアップデートはその手段や使用される環境をよく理解していないと想定外の事象を起こすことがある。

また、この事例とは直接の関係はないが悪意を持った攻撃者が、オンラインメンテナンスやアップデートの仕組を悪用し機器の動作や機能を変更するというタイプのリスクもあることの教訓にもなっている。

〈事例 5〉 医療機器システムの遠隔メンテのセキュリティホール

事象：セキュリティ系の某ベンダが提供する PC オンラインリモートコントロール製品を導入した医療検査装置において、そのリモートコントロールソフトのセキュリティホールにより、ネットワーク上から攻撃を受ける可能性が指摘され、製品回収に至った。

背景：

・機器のオンラインメンテナンスや操作法コンサルティング等を行うためのリモートコントロール機能は便利だが、攻撃対象となる可能性がある。特に本件のように安全にかかわる医療機器の場合には大きなリスクを想定しなければならず、慎重な対処が必要である。

開発ベンダの留意点：

・システム構築やメンテナンスサービス提供の技術的な選択肢として商用のリモートコントロール機能（ソフト）の組み込みを検討することがあるが、製品供給者のビジネストークを鵜呑みにすることなく、システムトータルのセキュリティ確保を十分に検討する必要がある。

〈事例 6〉 自動車制御装置の乗っ取りリスク

事象：米国のクライスラー社（FCAUS 社）は、2015 年 7 月に、同社の一部自動車車種がサイバー攻撃（遠隔操作）リスクの可能性を示唆されたとして、製品回収を発表した。

背景：

・IT メディアが、セキュリティ熟練者に協力を依頼して行った実験で、走行中の車を

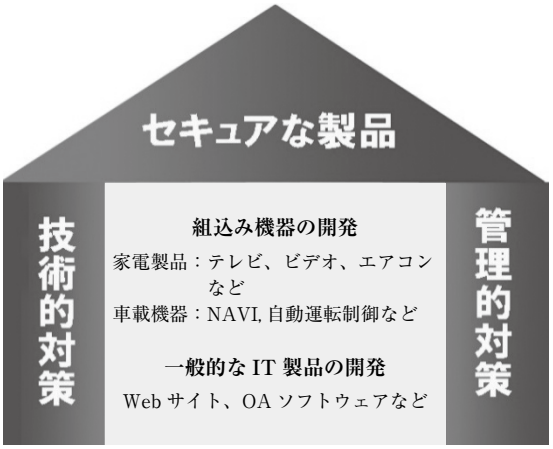
遠隔操作（ワイパー動作とエンジン停止）することが可能だったと報じた。実際に悪意ある攻撃を受けたという報告はないが、予防的な措置としてリコールに踏み切ったという。

開発ベンダの留意点：

・安全に関連するクリティカルなシステムでは、最終製品のメーカに協力して、十分なリスク分析のもと、十分なセキュリティ配慮をした実装を行う必要がある。

7　終わりにあたって

以上述べて来たように情報のセキュリティの確保ではいかなる対応策（管理策）を取るかが肝になるが、その場合、技術的対策だけでなく開発にまつわる人的・組織的・物理的[3]側面でのいわゆる管理的対策にも十分留意することが重要である。万全の技術的対策と日々改善を目指す管理的対策が、セキュアな製品を作り出す二本の柱であることを忘れてはならない。



■巻末参考資料

資料 1. 代表的なリスク分析のアプローチと手法

リスク分析手法として言及されることの多いものを下記に示す。

1）ベースラインアプローチ

既存のセキュリティ標準、基準やセキュリティ対策推奨策（これらをベースランと言う）をもとに、自社の実態とそれとのギャップをリスクとして評価するアプローチ。社会的な標準や基準を基に自組織の対策基準を策定し、その自組織基準と実態とのギャップをチェックしていく方法もある。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合が多い。また、現在、公式にはあまり推奨されない。

2）非形式的アプローチ

組織の熟練者や経験者、またはコンサルタント／学識経験者などの知恵を集めて経験、判断によりリスクアセスメントを行う。短時間に実施することが可能であるが、組織内の経験者等だけで実施すると、属人的な判断に偏る恐れが相当に大きい。

3）詳細リスク分析

データ、尺度を用いた評価表や数式を利用して詳細なリスクアセスメントを実施する。その例として次の表のようなものが挙げられる。セキュリティ要求事項を正しく理解するには、これらについてのある程度の知見があることが望ましい。

	手法名称	解　説
(a)	ISMS が基本とするアプローチ	情報資産を列挙し「資産価値（被害時の影響評価）」「脅威評価」「脆弱性評価」を行い、それを総合してリスクを評価していく。
(b)	FTA 法的なアプローチ	重要想定事故の原因となる事象を系統的に分析し、それに基づいて、事故の発生確率等を評価する。
(c)	ETA 法的なアプローチ	セキュリティ事故の進行と波及・拡散を系統的に評価する。セキュリティ分野でアタックツリーという手法が用いられることがあるが、上記の FTA 法や ETA 法に分類できる。
(d)	FMEA 法的なアプローチ	システムの構造を用いてシステム全体のリスクを評価する。可用性の評価に用いることが多い。
(e)	HAZOP 法的なアプローチ	定性的な異常事態評価語（ガイドワード）を用いてリスクの進行を評価する
(f)	形式手法	セキュリティ要求事項を数学的に厳密に記述し、要求事項の矛盾や抜け／漏れを低減・防止する。
(g)	実測・実験による評価	セキュリティテスト結果や、運用のユーザビリティ実験評価などの結果をセキュリティ要求にフィードバックする

(b)－(e)については、JIS C 5750 シリーズを参照。

3　物理的管理には、フロア入退管理や媒体持ち出し管理等が含まれる。

4）組合せアプローチ

複数のアプローチの併用。よく用いられるのは、⑴ベースラインアプローチと⑶詳細リスク分析の組合せである。ベースラインアプローチでギャップが大きい、あるいは疑問点があるセキュリティ課題について重点的に詳細リスク分析を行うなどする。

資料 2. 認証制度等の例

1）情報セキュリティマネジメントシステム適合性評価認証制度（ISMS）

個別の問題毎の技術対策の他に、組織のマネジメントとして、国際的な評価基準 ISO/IEC 27001(JIS Q 27001) に準拠して自らのリスクアセスメントにより 必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用する企業活動を認証する制度。

認定機関： JIPDEC

2）情報セキュリティ対策成熟度評価認証制度（CMSiS）

上記 ISMS 同様に ISO/IEC 27001（JIS Q 27001）に準拠した小規模な組織を対象とし、ISMS より簡素化されつつも実践的な運用ができる。チェックシートを用いて企業活動の実施面を認証する制度。

認定機関：JASA

組織面の情報セキュリティではなく本稿でとりあげている製品面のセキュリティ評価スキームとしては次のものがある。

3）コモンクライテリア認証制度（CC 認証）

情報システムを用いた製品やシステムについて、充分なセキュリティ対策が施されていることを評価する基準である ISO/IEC 15408（JIS X 5070）により、セキュリティ上の脅威を排除するための対策が充分に行われているかを審査する。

CC 認証は、製品ごとに行われるものであり、また厳密なものであるので、認証取得実施は重荷だと感じられる面がある。しかし、内容として参考とすべきものは多い。

認証機関：IPA

さらに、セキュリティ対応のための組織のプロセスの評価として次のものがある。

4）SSE-CMM (Systems Security Engineering Capability Maturity Model) 規格

セキュリティエンジニアリングプロセス成熟度評価の国際標準（ISO/IEC 21827）である。

5）国際標準である SPICE アセスメントのセキュアシステム開発プロセスへの適用

現在、ISO 等で審議中の国際標準がある。

6）VSE+SS 基準

本稿作成の背景として、小規模開発組織向けのセキュアなソフトウェア／システム開発の基準を VSE+SS 合同研究会で開発中である。VSE とは、小規模開発組織向けの開発プロセスの国際標準で、コンパクトなプロセス群を提示しているが、それに開発対象のソフトウェアのセキュリティとセーフティ（安全）の側面を付加するための基準である。

資料 3. ライフサイクルにおけるセキュリティ施策の展開

製品の開発・運用では、セキュリティのリスク分析に基づいて必要なレベル感で実務を進めていく。その際に、それぞれのプロセスで具体的には次のようなことに留意する。これらについて、発注側と受注側の責任範囲を明確にし、情報交換も緻密に行う。

1）企画・設計時点

・どのようなユーザ種別を想定し、それに応じたどのようなアクセス制御を行うかの方針を決める
・電子署名やパスワードを用いる場合、それらのシステム上、運用上の管理をどのように行うかを決める。
・ユースケースなどに基づき、セキュアな運用が確保されているか検討し決定する。
・セキュアなコンポーネント、ライブラリ等の採用を決定する。

2）詳細設計・実装時点

・暗号関連処理の実装をどのように行うか（場合

により、暗号化対応は専門家の参画が必要)。
・セッション管理をどのように行うか。
・直接オブジェクト参照などの脆弱性をどのように防止するか。
・同時アクセス制御を確実に行う（レースコンディションやデッドロックの確実な回避を含む)。
・データ検証処理、及び各種のエラー処理をセキュアに行い（フェールセーフ処理を含む)、また攻撃者がエラーメッセージから容易にシステム特性を把握できないようにする。
・セキュア・プログラミングを確実に実行する（コーディングルール策定や、その順守状況チェック)。

具体的な内容としては、バッファーオーバーフロー対策、フォーマットストリング対策、コマンドインジェクション対策、セッション管理対策等がある。

3）テスト時点

・ペネトレーションテストの手法と範囲を検討する。
・既知の脆弱性に対するチェック方策を検討する。
・運用におけるセキュリティ上の留意点が確実にテスト範囲に含まれるようにする。

4）リリース時点と運用時点

・リリースノートにセキュリティ上の注意事項が確実かつ有効に記載されるようにする。
・運用時の過去の不具合情報を教訓として活用する。
・セキュリティパッチの作成・配布方法について明確にする。可能な場合、IPA と JPCERT/CC が運用している脆弱性取扱いスキームに整合させる。

資料 4. 組織名の略語等の表

IPA	(独）情報処理推進機構
JASA	(一社）組込みシステム技術協会
JIPDEC	(一財）日本情報経済社会推進協会
JPCERT/CC	(一社）JPCERT コーディネーションセンター
OWASP	Open Web Application Security Project
CERT	米国カーネギーメロン大学のセキュリティインシデント対応・研究部署の名称（略語ではない）

資料 5. 参考資料

1）JIS Q 27001：2014
2）Official（ISC）2 Guide to the CSSLP", CRC Press（2011）
3）IPA「2013 年度　医療機器における情報セキュリティに関する調査」(2014 年 4 月刊）

[解説]
セーフティの基礎
～ VSE への展開にむけて～

足立 久美、田渕 一成
VSE+SS 合同研究会一同

キーワード

VSE、セーフティ、リスクアセスメント、本質的安全、機能安全、ISO/IEC GUIDE 51、ISO 26262、Automotive SPICE、セキュリティ

要　旨

今日、我々は様々な製品やサービスの恩恵を受けているが、逆にその欠陥や障害等により不利益を被ることもある。特に「社会とつながる」という機能をもった製品やサービスは、一度の障害が社会に大きなダメージを与えかねない。エンジニアはこのことを肝に銘じて、安全・安心な製品やサービスを利用者に提供していかなくてはならない。これを実現するための重要なキーワードは、セーフティ（Safety：安全性）とセキュリティ（Security）である。本稿では、VSE（Very Small Entities：比較的小さなソフトウェアを開発する小規模な組織）が、製品やサービスのセーフティとセキュリティに関する設計活動を見直すのにあたり、セーフティについて必要最低限知っておくべきこと、および車載電子システムにおける安全の動向や課題から得られたセーフティの適用のヒントについて解説する。

1　はじめに

我々の生活は、自動車、鉄道、航空機などの乗り物、電気、ガス、水道、銀行のオンラインシステムなどのインフラ、家庭における様々な電化製品など、日常のあらゆる場面でソフトウェア技術の恩恵を受けている。

一方、近年はソフトウェアを搭載した製品やソフトウェアを用いたサービスの大規模化、複雑化に伴い、ソフトウェアの欠陥により、その利用者が身体的な危害や経済的な損失を受ける事案も度々発生しており、ソフトウェアの安全・安心への関心が急速に高まっている。このように、ソフトウェア技術（エンジニアリング）は、我々に利便性や快適性を提供してくれる半面、使い方を誤れば製品やサービスの利用者に対して害をもたらしかねないのである。つまり、ソフトウェアを搭載した製品やソフトウェアを利用した製品やサービスの提供者である技術者（エンジニア）は、所属する企業や組織の規模に関わらず、このことを強く認識し、安全な製品やサービスを社会に提供していかなければならない。

ここで、安全な製品やサービスを提供するということは、単に品質が高いということや信頼性が高いということとは同一ではないという点に注意して欲しい。「安全」という言葉と対としてよく使われる言葉に「安心」という言葉があるが、安全とは製品やサービスを利用する人にとっての安心につながるものでなければならない。つまり、製品を開発した本人がその安全性にどれだけ自信

を持っていても、それを利用する相手にその安全性が理解されなければ、相手にとっての安心にはつながらず、安全性を保証したことにはならない。そのため、安全性は製品やサービスの利用者、またはその開発を委託した委託元にとって、理解可能な形で示される必要があり、安全性を裏付けるエビデンスを確実に構築していくことも重要視される。

本稿では、特にVSE（Very Small Entities：比較的小さなソフトウェアを開発する小規模な組織）が製品を開発していくにあたり、必要最低限知っておくべきことをセーフティの側面から、第2章で、「安全設計の基本」として主に「安全設計の考え方」と「リスクアセスメント」について平易に解説する。また、第3章で、「VSEへの適用にむけて」と題して、車載電子システムにおける安全の動向と課題に基づいて、セーフティのVSEへの適用のヒントを探っていく。

2　安全設計の基本

本章では、安全設計とリスクアセスメントの考え方について述べる。

2.1　安全設計の考え方

安全設計とは、「ものは壊れる、人はミスをする」ことを前提にし、その防止策や被害の最小策を設計に盛り込むことである。

誤操作等の不具合要因が発生した場合でも、人・財産・環境への危害が出ないように防護策を施す必要がある。しかしながら、完全な防護策を構築することは難しく、何らかのリスクが残留する場合が多い。そこで、単一の不具合による直接的な危害を発生させないために、図1のように多重防護策を設ける必要がある（図1の防護壁が防護策にあたる）。

図1はマンチェスター大学の心理学教授ジェームズ・リーズンによって1990年に提唱されたスイスチーズモデル（Swiss cheese model：SCM）である。このモデルは、不具合要因が多重の防護策の穴をすべて潜り抜けた場合に危害が発生することを示している。一方で、このモデルは同一の原因により複数の防護策を脅かしてはならないことの重要性を示している。

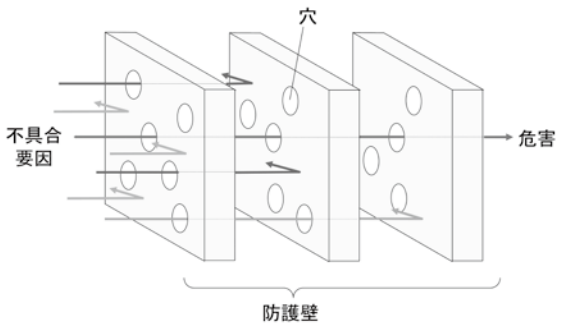


図1　スイスチーズモデル
James Reason（1990）

そこで、安全設計における代表的な防護策として、フールプルーフ（Fool Proof）とフェイルセーフ（Fail Safe）について以下に紹介する[1)]。エンジニアは、少なくともこの二つの防護策を理解し両者の違いを識別できなければならない。

（1）フールプルーフ（Fool Proof）

人は間違うことを前提にし、間違えにくい設計または、間違うことの出来ない設計をすることをフールプルーフと言う。

これは、図2の防護壁（A）に該当する。操作ミスなど人が誤った機械操作を行えば、機械装置が人に危害を与える可能性が考えられる場合、人が操作を間違えにくい設計または、人が間違うことの出来ない設計をすることが重要である。

フールプルーフは、通種バカヨケ、ポカヨケと呼ばれており、電池を＋－逆接できないようになっている電池ボックスなどがこれにあたる。

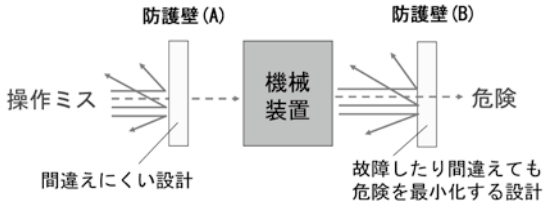


図2　フールプルーフとフェイルセーフ

（2）フェイルセーフ（Fail Safe）

もし間違いが発生しても、被害を発生させない、もしくは最小にとどめる設計をすることをフェイルセーフと言う。これは、図２の防護壁（B）に該当する。操作ミスなど人が誤った機械操作を行ったり、機械装置が故障しても、機械装置が人に与える危害を最小化する設計、例えば故障してもなお安全を保ったり、誤動作したり危険な出力を生じないようにする（回路故障の際に、できる限り安全側の出力をする）といった設計をすることが重要である。決められた上限の速度を超えてカーブに電車が入ってきた場合に電車を止める ATS などがこれにあたる。

なお、防護策には、一つのシステムを複数の装置に分散して処理させるなど、システムの一部が故障した場合に性能の低下をさせてでも機能を継続的に実施させるといった「フェイルソフト（Fail Soft）」や、航空機の与圧装置を２系統にするなど障害は必ず発生するという考えに立ちソフトウェアやハードウェアの冗長化をすることによりシステムの信頼性を図るといった「フォールトトレランス（Fault Tolerance：対故障性）」、製品やサービスの構成要素から可能な限り故障や障害などの不具合の発生要因を排除する、また不具合が発生しないように十分なテストを行うなど構成要素の信頼性を高めるといった「フォールトアボイダンス（Fault Avoidance）」がある。

2.2 リスクアセスメント

安全は、図３に示すように受入れ不可能なリスクをなくし、リスクを受容可能なレベル（受容可能なリスク）になるまで低減させることで達成される。つまり、このことは製品やサービスの安全性を担保するためには、その製品やサービスが、市場でどのように使用されるかを想定し、その使われ方に起因する危害を特定し、その危害のレベルを利用者が受容できるレベルまで下げればよいことを意味する。

ここで、「許容可能なリスク」とは、特定の条件下では受け入れることができるリスクのことである。また、安全に関する必ず押さえておきたい重要な安全関係の用語を表１に示しておく（国際規格 ISO/IEC GUIDE 51：1999 は 2014 年に ISO/IEC GUIDE 51：2014[2]として改訂された際に、「安全（Safety）の定義が「受容できないリスクがないこと」から「許容できないリスクがないこと」に改正された。なお、「受容可能なリスク」とは、どのような条件下でも受入れることができるリスクをいう）。

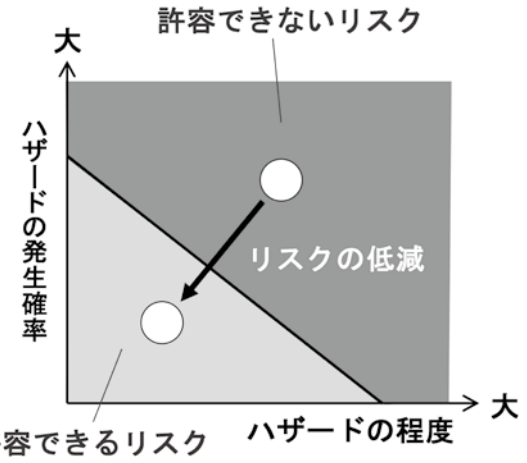


図３　許容できるリスクと許容できないリスク

【用語の定義】 ISO/IEC GUIDE 51: 2014より引用（和訳）	
危害(harm)	人の受ける身体的障害若しくは健康被害、又は財産若しくは環境の受ける害。
リスク(risk)	危害の発生確率及びその危害の程度の組合わせ。
ハザード(hazard)	危害の潜在的な源。起こる可能性のある危害の発生源又は性質を定義する。
安全(Safety)	許容できないリスクがないこと。

表１　安全に関連する重要な用語

安全を実現する方法として一般的に使われている方法がリスクアセスメントである。国際規格 ISO/IEC GUIDE 51：1999（JIS Z8051：2004）[3][4]では、「許容可能なリスクをリスクアセスメントによるリスク低減プロセスを反復することによって達成させる。」こととし、図４に示すようなリスクアセスメント及びリスク低減の反復プロセスを定義している。

ここで、国際規格 ISO/IEC GUIDE 51：1999 は 2014 年に ISO/IEC GUIDE 51：2014 として改訂された際に、リスクアセスメント及びリスクの

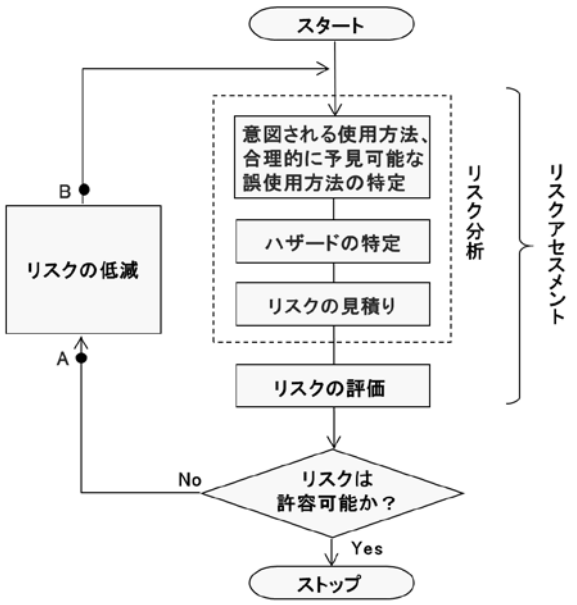


図４　リスクアセスメント及びリスク低減の反復プロセス
ISO/IEC GUIDE 51：1999（JIS Z8051：2004）より引用

低減の反復プロセスの図が詳細な図に変更されたが、本稿では旧版の ISO/IEC GUIDE 51：1999（JIS Z8051：2004）の図を用いた（理由：旧版と新版とでは基本的な考え方は変わらない。また、反復的リスク低減プロセスを３ステップメソッドとして詳細に定義している ISO 12100：2010（JIS B9700：2013）との対応をとるため）。

リスクアセスメント及びリスク低減の反復プロセス（図４）は、リスクアセスメントとリスクの低減により構成される。さらに、リスクアセスメントはリスク分析とリスクの評価により構成される。以下、これらについて順番に説明する。

（1）リスク分析

リスク分析は、さらに「意図される使用方法・合理的に予見可能な誤使用方法の特定」、「ハザードの特定」、「リスクの見積り」により構成される。

まず、最初に対象の製品やサービスの意図される使用方法と予見可能な誤使用方法を特定する。一般的に、「意図する使用方法を特定すること」よりも、「予見可能な誤使用を特定すること」の方が開発者にとって比較的難しい。また、予見可能である限り事故発生時の責任はメーカーが負うべきという考え方があるため、この予見可能な誤使用を特定することが重要なポイントである。

ここで、予見可能な誤使用とは、開発者（メーカー）が推奨する使用方法でないにも関わらず、使用者の都合によって採用されてしまう誤った使用方法のことである。これは、通常はロックをかけて使用するようにメーカーが指定しているにも関わらず、使用者自身がロックを解除して使用することで操作の手間が軽減されるといった場合など、使用者が何らかの利点を感じることにより採用してしまうことが多く、それに伴って危険な事象を発生させることがある。以上のことから、メーカーは意図しない使用方法であっても、使用者が故意に採用する可能性のある使用方法も含めて、予見可能な範囲における全ての使用方法を特定しなければならない。

次に、特定した各使用方法に対して個々に発生するハザードを特定する。代表的なハザードの特定方法に FTA、FMEA、HAZOP がある。

最後に、その発生するハザードが引き起こす製品やサービスの使用者や関係者に対するリスクを見積る。リスクの見積りでは主に危害の程度と発生確率の算定を行う。

（2）リスクの評価

リスクの見積りが終了したら、それが許容可能であるか否かリスクの評価を行う。もし、許容可能であればプロセスを終了する（終了に際して結果の妥当性確認をすることが望ましい）。許容可能でなければ「リスクの低減」を図った上で最初に戻り、リスク（残留リスク）が許容可能となるまで反復する。なお、「リスクの低減」を反復しても、リスク（残留リスク）が許容可能とならない場合は、製品やサービスの開発の見直しをする必要がある。

ここで、リスクアセスメントではリスクを「許容可能なレベル（許容可能なリスク）まで低減する」とあるが、できれば「受容可能なリスク」までの低減を狙うべきである。

（3）リスクの低減

図５に「リスクの低減」の方法を示す。「リスクの低減」方法は図に示すように、さらに「本質的安全設計方策」、「安全保護（保護装置）」、「安全上（使用上）の方法」の３つのリスクの低減方法により構成される。

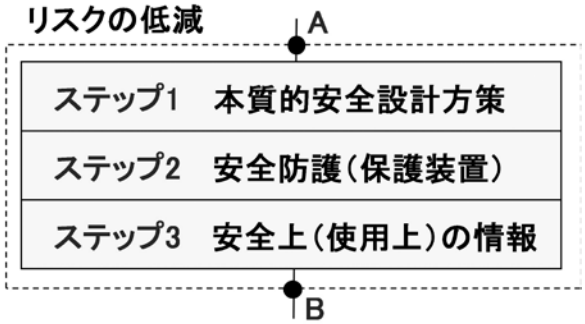


図５　リスクの低減手段（保護方策）
ISO/IEC GUIDE 51：2014 より引用

リスクの低減で最初に実施するのは、「危険源をなくす、または無くせない場合は危険源のリスクを低減する。」といった本質的安全設計である。本質的安全設計の実例を図７に記す。図７では自動車道路と鉄道を立体交差にすることにより本質的安全設計をしている。

図６　本質的安全の例：立体交差

図７　安全防護の例：遮断機付きの踏切

その次に、本質的安全設計を実施してもまだ許容できない残留リスクがあれば、「安全防護（保護装置）をつけて低減する」といった安全防護（保護装置）による防護を行う。ここで、前節で解説したフールプルーフやフェイルセーフがこの安全防護の方法に相当する。

安全防護（保護装置）による防護の実例を図７に記す。図７では自動車道路と鉄道が交差するところに、地形等の理由で本質的安全設計（立体交差）にすることができない場合に、安全防護（保護装置）として遮断機付きの踏切を設置している。

そして、最後に安全防護（保護装置）を実施してもまだ許容できない残留リスクがあれば、「使用上の情報を使用者に伝える」といった使用上（安全上）の情報発信を行う。図７では警報機（踏切の存在を通行者に知らせる踏切警標、列車の接近を視覚的に警告する警報灯、列車の接近を音により知らせる警報音、踏切が危険区域であることを示す、黄色と黒の縞模様の警告色がこれに相当する。

ここで、特に注意して欲しいことは、３つの方策には優先順位（図中の番号）があるということである。つまり、本質的安全設計を考慮せずにいきなり安全防護によりリスクの低減をするのではなく、本質的安全設計をした上で残留リスクがあれば、安全防護をとるべきである。

なお、国際規格 ISO 12100：2010（JIS B9700：2013）[5)6)]の「リスクの低減」の３つの方策の定義を表２に記しておく。

【用語の定義】　ISO 12100:2010　(JIS B9700:2013)より引用	
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って、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
安全防護 (safeguarding)	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
使用上の情報 (information for use)	使用者に情報を伝える伝達手段(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

表２　リスクの低減の３つの方策の定義

図８　本質的安全の例：立体交差（その２）

ここで、次の設問の答えを考えて下さい。

設問：図８は図６に対して線路と道路が上下逆なだけで、同じ本質的安全の例であるが、一つの違いがある。それは何ですか？

答えは、図８では道路側に安全防護策として、鉄道のガード下に車が衝突し橋脚にダメージを与えないようにする衝突防止のためのゲート（線路の橋脚囲い）があることである（図中の鉄製で頑丈な黄色の構造物で、鉄道のガード下の高さより衝突防止のためのゲートの高さが低く設定されている）。これは、先に説明したフールプルーフ（線路の橋脚に衝突させない）に相当する防護策です。逆に図６には衝突防止のためのゲートがないのは、線路を走る電車はその車高を確実に制限できるためである。しかしながら、自動車（特に特殊車両）は確実に車高を制限することができない。図８は、このことも想定し本質的安全と安全防護の両方の対策をしていることを示している。なお、この衝突防止ゲートにも図７の踏切と同様に黄色と黒の縞模様の警告色をつけて、危険区域であることを視認し易くしている。

以上、３つのリスク低減手段について述べてきたが、これらは設計者によって講じられる保護方策に関するものである。ISO/IEC GUIDE 51：2014 には、製品やサービスの使用者にとっての安全活動を「使用者によって講ずる保護方策」として定義している。これを図９に示す。

製品やサービスの利用者は、使用上の情報をもとに、防護装置を追加したり、訓練をしたり、保護具を装備するといった活動を実施することになる。

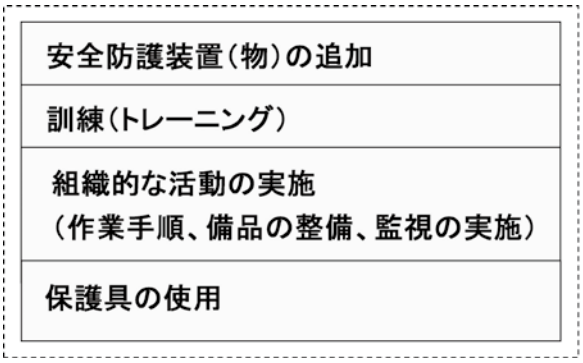


図９　使用者によって講ずる保護方策
ISO/IEC GUIDE 51：2014 より引用

いくら設計者側が安全活動、安全設計によって許容可能なレベルまでリスクの低減をしたとしても、利用者側においても安全活動を実施し、さらに残存リスクを軽減することは大切である。絶対的安全というものはありません。設計者側はもちろんですが、利用者側も安全意識、危機意識を持ち続けることが肝要です。

2.3　機能安全とは

近年、車載電子システム向けの機能安全規格「ISO26262」[7]などにより「機能安全」という言葉をよく耳にする。ここでいう「機能安全」は、「リスクの低減」の３つの方策の中の「安全防護（保護装置）」に相当する。

本稿では、機能安全についての詳細な解説は省略するが、機能安全を理解する上で重要な用語の一つである「安全文化」について以下に説明をしておく。

「安全文化」とは、組織およびそれに属す個人に根付く安全の考え方や行動指針である。

安全文化の必要性が強く求められるきっかけとなったのが、1986 年のチェルノブイリの原子力発電所の事故である。この事故において、国際原子力機関がその原因を調査していく中で、現場の作業員、発電所を運営する事業者、行政などそれぞれに安全に対する考え方や仕組みの問題が提起

され、安全文化の必要性が唱えられた。現場の作業員に安全管理のマニュアルが渡されていても、作業員がその本質を理解していない限り、安全管理は本来の効果が期待できない。また、組織においても安全管理者を設置するだけではなく、組織としての目標を掲げ、それを実現するための仕組みや人材の育成が求められる。

これは、車載電子システムの開発においても同じことが言える。後述の 3.1 にも関連した事象を述べているが、ISO 26262 や Automotive SPICE[8]の対応が求められたことによって、プロセスの定義やガイドラインの作成を形だけの対応で終わらせようとするケースも世の中には見られるが、これでは安全文化の醸成は難しい。そのような組織の中には、上層部が安全の重要性を理解しておらず、最小の努力で規格対応を終わらせるよう指示をしてしまっている場合も見受けられるが、改めて機能安全対応の本来の目的を考えるべきである。

また、機能安全対応の当初は明確な目的を持ってプロセス構築がされたものの、それが組織内で使用されていく中で、組織標準プロセスの構築当初の意図が忘れ去られ、結果的に不遵守へと陥るケースもある。人は誰でも意味のない活動を好まないものであり、意図のわからない活動は定着しない。そのため、組織標準プロセスは一度構築して終わりではなく、組織の中で絶えず改善を続け、組織標準プロセスを継承していく必要がある。

さらには，製品設計における安全を最優先する風土や気風の形成が，安全文化の醸成において非常に重要である。具体的に言えば、安全最優先の価値観（例えば組織の安全方針や目標）が関係者全員で共有され、その共有された価値観に従って日々の設計業務（例えば、組織の安全方針や目標を満足又は達成する安全活動）が遂行されていることが要求される。いくら良い技術やプロセスがあっても、安全文化が未成熟な組織では、安全・安心な製品やサービスを継続的に利用者に提供していくことは難しい。

安全文化が成熟している組織では、組織を構成するメンバーのより安全・安心な製品・サービスを提供しようとする姿勢（使命感）、円滑なコミュニケーションによる情報共有（特に悪い情報）、同じ失敗を繰り返さない振り返り（学習）活動、決められた基準・ルールの遵守などがアウトカム（outcome）として観測される。

2.4 安全関係の国際規格について

安全に対する国際規格は、表 3 に示すように、安全性に関する基本的な概念・原則・要求事項を規定した「基本安全規格」、複数の製品・サービスの安全性を規定した「グループ安全規格」、個別の製品・サービスの安全性を規定した「製品安全規格」といった複数の規格で構成されています。

分類	説明	解釈
基本安全規格	広範囲の製品，プロセス及びサービスに対して適用する一般的な安全側面に関する基本概念，原則及び要求事項を含む規格．	普遍的な安全の基本概念や原則． 機械類の安全性―設計のための一般設計原則であるISO 12100など
グループ安全規格	一つ又は複数の委員会が取り扱う幾つかの又は一群の類似の製品，プロセス及びサービスに適用できる安全側面を含む規格．	機械，電気の安全や，機能安全など，特定の技術分野における安全の基本概念，機能安全のIEC 61508など
製品安全規格	一つの委員会がその業務範囲内で取り扱う特定の又は一群の製品，プロセス若しくはサービスの安全側面を含む規格．	特定の製品分野における安全の要求． 車載システムにおけるISO 26262など

安全に関する規定を規格に導入するためのガイドラインISO/IEC GUIDE51から抜粋し解釈を加筆

表３　安全規格の種類

本稿で主に参照した規格は、二つの国際規格「安全側面－規格への導入指針：ISO/IEC GUIDE 51：1999（JIS Z8051：2004）」と「機械類の安全性―設計のための一般設計原則－リスクアセスメント及びリスクの低減：ISO 12100：2010（JIS B9700：2013）」である。安全設計に関わるエンジニアは少なくともこの二つの国際規格は読んでおかれることを強く推奨する。

車載電子システムの分野においては、2011 年に機能安全規格 ISO 26262 が発行され、完成車メーカーと自動車部品メーカーを中心にその取り組みが行われてきている。

この規格は、前述の ISO/IEC GUIDE 51 の体系の中に位置づけられ、基本理念を引き継ぎつつ車載電子システムの特徴に基づいて構築された。しかしながら、ISO 26262 は、IEC 61508 等の従来の機能安全規格のアプローチに加え、車載電子システムの開発の分野で取り組まれてきたプロセ

スアプローチをその土台として色濃く持っている。

ここで簡単にISO 26262の発行に至るまでの車載電子システム開発発の分野での取り組みを解説する。

1990年代の後半から2000年代の初頭にかけ、自動車のエレクトロニクス化が急速に進み、車載電子システム開発の環境が大規模かつ複雑なものへと変化した。特に、車載電子システムに搭載されるソフトウェアの開発においては、前述の大規模化、複雑化に伴い、開発の受委託関係を含めた開発体制にも大きな変化をもたらした。その結果、ソフトウェアに起因した不具合が急速に増加し、その対策が重要視され始めたのである。特に、自動車としてのもっとも基本的な機能である走る・曲がる・止まるという機能におけるエレクトロニクス化は、それに起因した不具合が発生することで自動車の運転手や同乗者、周囲の歩行者の安全を脅かすこととなる。

このような状況の中、図10に示すように、2000年代の初頭から欧州の完成車メーカーを中心に、車載電子システム向けの機能安全規格の必要性が訴えられ始め規格の策定につながっていった。

この車載電子システム向けの機能安全規格の策定に向けた動きと平行して、品質の向上のため開発委託先に対するプロセスアプローチを強く推奨する動きが始まっていった。当初は、各完成車メーカーが独自の基準に基づいた取り組みを展開していたものの、開発委託先の品質向上は完成車メーカー共通の課題であったため、2005年には、ISO/IEC 15504やISO/IEC 12207に基づいて、

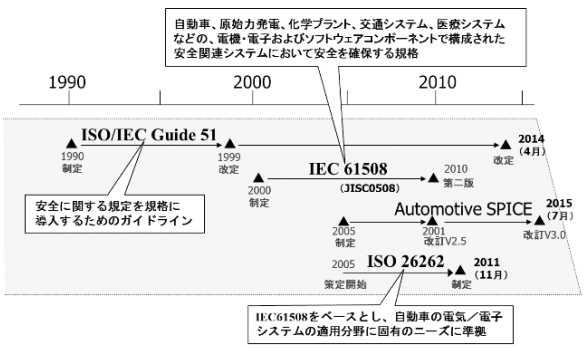


図10　車載電子システムの安全に関する規格の推移

車載電子システム開発向けのプロセスアセスメントモデルとしてAutomotive SPICEが策定された。

従来の車載電子システム開発の分野では、CMMIやISO/IEC 15504に基づいて自社のプロセス改善に取り組む動きもあったが、それらのモデルや規格と比較して、Automotive SPICEは、開発委託先に対して開発委託元が第二者の立場でアセスメントを行うための特徴が強く反映されている。

そしてまもなくAutomotive SPICEは、欧州を中心として完成車メーカーの調達要件として掲げられるようになり、これに基づくプロセスアプローチは、車載電子システムを開発する上で広く適用されるようになっていった。

このようにAutomotive SPICEは、ISO 26262が発行される以前から車載電子システム開発の品質向上のために広く適用されるようになっており、その存在はISO 26262の策定や活用の仕方にも大きな影響を与えた。逆に、Automotive SPICEもISO 26262の影響を受け、改定が進んだのである。つまり、この両者は非常に密接な関係を持つようになり、車載電子システム開発の分野においては、多くの場合、この両者の対応が同時に求められている。

ISO 26262が発行された当初は、規格の解釈が十分でなかった場合などもあり、Automotive SPICE対応のための組織標準プロセスとISO 26262対応のための組織標準プロセスを別々に構築している組織も見受けられたが、本来の組織標準プロセスとは、組織のあるべき姿を反映したものであり、Automotive SPICEやISO 26262の対応要求に左右されるものではない。

3　VSEへの適用に向けて

3.1　安全設計のVSEへの適用の考察

これまで述べてきた車載電子システム開発の分

野における動向や課題に基づいて、VSE への適用について考察する。

一般に、車載電子システムに搭載されるソフトウェアの開発は、非常に大規模なプロジェクトで行われているという印象を持たれている方も多いが、カーナビゲーションシステムなど一部のシステムを除けば、大手の自動車部品メーカーにおいても、実際には 10 人以下の小規模なプロジェクトが全体の半数以上を占めている。しかしながら、プロジェクトの規模に関わらず、安全な製品を開発するという責任は変わるものではなく、車載電子システムの開発の委託元である完成車メーカーからは、前述の ISO 26262 や Automotive SPICE の対応が厳しく求められているのである。

自動車の分野においても、プロジェクトの規模が小さいため、ISO 26262 や Automotive SPICE の対応が難しいという旨の声が聞こえることもあるが、これらの規格やモデルの対応において重要視されていることの一つが、組織の特性に合わせた組織標準プロセスの構築と、プロジェクト特性に合わせたプロセスのテーラリングである。つまり、ISO 26262 や Automotive SPICE の対応は小規模なプロジェクトにとって必ずしも負荷の高いものということではなく、安全なものづくりを適切に行っていく上で、組織やプロジェクトの特性に合わせて取り組むべきこと、そして説明責任を果たすことが求められているだけとも言えよう。確かに、中小企業よりも大企業の方が、組織内に安全活動を推進するための間接部門を置いたり、広く知見の共有を行ったりすることのできる利点はある。しかしながら、安全なものづくりをする上で果たすべき責任は、組織の規模に関わらず同じである。

3.2 安全設計の経験に基づく VSE に向けたヒント

最後に、機能安全対応にありがちな 5 つのケースと、VSE での対応のヒントを考察する。

(1)「国際規格や法規の遵守」だけを目的としているケース

結論から述べると、国際規格や法規を遵守すれさえいれば、安全な製品を開発できるわけではないということである。

規格や法規への対応は、下記の 3 つに区分することができる。

- 法規（国家や国家連合体）で規定されている安全要求
- 顧客（OEM）の会社規程（標準等）で規定されている安全要求（国際規格から引用したもの及び自社独自の規程）
- 自社規程（標準）で規定されている安全要求

まず、法的な要求は必ず満足しなければならず、また顧客からの安全要求も RFQ（Request for Quotation：見積依頼書）や SOW（Statement of work：作業明細書）等で合意した以上満足しなければならない。さらに自社規程からの安全要求も含めて、これらの安全要求は、遵守すべきことの最低ラインとしての要求であり、これらを満足することが最終目標となってはならない。もちろん、正当な理由がある場合はその理由を明確に残した上でテーラリングをすればよい。（法規を除く）

また、国際規格には何をするべきか（what）は書かれているが、どのように実現するのか（how）まで書かれていないことが多い。なぜならば、前述のように、これらの要求事項は最低ラインとしてのものであり、その手段を詳細に要求するものではないからである。

さらに、国際規格は、必ずしも実施順序どおりに記載されていないことがあるので注意が必要である（国際規格をそのまま自社ルールに張り付けてもうまくいかない）。また、一般の開発者にとって、要求の意味が十分に理解できないものや、要求されている技法の適用の際の厳格さまでは記載されていないことも多く、関連規程や参考資料を参照しながら準備に膨大な時間を費やさなければならない場合もある。前述のように、国際規格はあくまでも遵守すべき最低ラインの定義であり、それを自社の製品やサービスにあてはめな

がら最適化し、組織の規程（標準、ルール、手順など）に確実に実装していくことが肝要である。つまり、規格に書いてある通りやコンサルタントに言われた通り実施するのではなく、自分の頭で目的を考えることが重要である。

（2）「安全活動＝安全防護（機能安全）」と考えているケース

第２章のリスクアセスメントで説明した３つのリスクの低減方策の中の安全防護（機能安全）のみを安全活動と位置づけ、安全防御（機能安全）に特化した安全活動をしているケースも見られる。(1) のケースの国際規格に準拠しさえいれば良いというケースにおいて発生することが多い。安全設計のリスクの低減において、最初に考えるべきは「本質的安全設計」である。

しかしながら、本質的安全設計はソフトウェアだけでは対応することが出来ない。製品のシステム全体で安全性を考慮して初めて本質的安全設計が可能となるのである。そのため、ソフトウェアエンジニアの中にはシステム全体の安全性を考慮すること自体を不可能と捉えている場合も見受けられるが、システム全体の考慮なしではソフトウェアの安全上のあるべき振る舞いは見出すことができない。

（3）認証取得だけを目的としているケース

プロセス認証、ツール認証などの認証を取得することが、安全活動の目的になってしまっているケースがある。安全活動の目的は認証を取ることではなく、自社が利用者に提供する製品やサービスの安全性を確保することである。また認証機関が対象製品の安全性そのものを保証するものではない。

一般に、認証は以下の２つの理由により対応が求められる場合が多い。

- 流通対象国の法規要求や顧客要求で指定されている。
- 顧客に自分たちの提供する製品やサービスの安全性を効果的に主張する根拠として用いる。

なお、認証の取得や認証の維持にはそれなりのコストが必要となるため、やみくもに認証を取得するのではなく、認証を取得することの効果をよく考えた上で決断すべきである。

（4）技術者倫理感が乏しくなったケース

「機能安全の国際規格への対応が要求されたから、これから安全設計をしなければいけない。」という趣旨の発言をしているケースのことである。そもそも、セーフティへの取り組みは、機能安全の国際規格が発行されて初めて取り組むものではなく、従来から社会に対して製品やサービスを提供してきた企業であればすでに自社の安全文化が築かれ、自社の提供する製品やサービスに安全設計を施しているはずである。もし、そうでなければ安全対策が不十分な製品やサービスを社会に供給していることになってしまう。機能安全規格への対応だけが目的となってしまっている企業の中には、前述のようにこれから初めて安全対策、安全設計を行うような感覚を持っているエンジニアも少なくなく、規格の対応から外れた製品については、安全設計が不要という考え方も見られる。そのような企業は、機能安全規格への対応の前に技術者倫理の教育を行い、企業の社会的責任を果たす企業の風土を構築する必要がある。製品設計と安全設計は表裏一体である。

（5）「苦能安全」活動と捉えてしまったケース。

「機能安全の国際規格への対応が要求されたので、これから大変だ！」といった考えに陥っているケースである。(4) でも述べたように、安全文化の醸成も安全設計も一から始めるわけではなく、組織がそれまで蓄積してきた基盤がある。適切な安全活動を実施しているのなら、その基盤（ベース）に自信をもって、「機能安全の国際規格への対応が要求されたので、自分たちが従来からやっている安全設計を、国際基準に照らし合わせて、どのように準拠しているかの説明責任を果たせばよい。もし、不十分な点があれば必要な改善をおこなっていけば良い。」と考えるべきである。

この考え方こそ「喜能安全」活動である。

また、機能安全の対応は必ずしも工数の増加を招くものではないということに着目する必要がある。プロセスアプローチが機能安全対応の土台と前述していたが、適切なプロセスの適用は、全体として大幅に効率が向上する。それぞれが個人のノウハウに基づいて独自の開発をしていた状況では、それぞれの成果物に対して、その内容の正しさや妥当性を客観的な立場から裏付けることは容易ではないが、開発活動が組織の標準プロセスに基づいて展開され、計画の逸脱がないことを常に監視し、標準化された手法に基づいて開発を行い、成果物を客観的に評価するための仕組みが確立しているなど、適切なプロセスアプローチが行われることで、開発の効率化だけではなく、組織へのノウハウの蓄積、さらには、安全文化の醸成が期待される。

4 まとめ

以上まとめると、セーフティへの取り組みにおいては、組織の規模に関わらず安全文化の醸成がもっとも重要と言えよう。

製品の開発に関わるエンジニアは、安全文化の重要性を理解する必要がある。そのためには、エンジニアはスリーステップメソッドに従ったセーフティの基本アプローチと安全技術の基本原理を十分に理解する必要がある。

また、組織は安全な製品を開発するための組織の特性に合ったプロセスを構築する必要があり、さらに個別の開発プロジェクトにおいては、プロジェクトの特性に合わせて組織標準プロセスを仕立て直すテーラリングが必要である。

このように、組織、プロジェクト、個人のそれぞれの役割を果たすことで初めて安全文化が醸成されるのである。

従来は、安全・安心な製品やサービスを自社基準で提供すれば良かったが、これからは製品やサービスが安全・安心であることを、客観的かつ具体的な証拠でもって利用者に説明するといった説明責任（Accountability）を果たさなければならない時代となった。安全とは、相手に対して安心を与えることなのである。自分自身がいくら安全に自信を持っていても、また自社の安全基準を達成していたとしても、それが相手にとって理解できるものでなければ、相手は安心しない、つまり、安全とは言えないのである。このような安全の説明責任は、大企業であっても、VSE であっても同じである。

今後は VSE が提供する安全・安心な製品やサービスにも、セーフティとセキュリティが問われる。取り組みはじめるのは今、「安全に手抜きなし」である。安全文化を醸成し、リスクアセスメントを活用するなど、より安全・安心な製品やサービスを提供していくことを期待する。

■文献

1）独立行政法人情報処理推進機構，組込みシステムの安全性向上の勧め（機能安全編），2006.
2）ISO/IEC GUIDE 51 Safety aspects – Guidelines for their inclusion in standards, 2014.
3）ISO/IEC GUIDE 51 Safety aspects – Guidelines for their inclusion in standards, 1999.
4）財団法人日本規格協会，JIS Z8051,「安全側面－規格への導入指針，2004.
5）ISO 12100 Safety of machinery – General principles for design – Risk assessment and risk reduction, 2010
6）財団法人日本規格協会，JIS B9700，機械類の安全性―設計のための一般設計原則－リスクアセスメント及びリスクの低減，2013.
7）ISO 26262 Road vehicles - Functional safety, International Standard, first edition, 2011.
8）Automotive Special Interest Group：Automotive SPICE（R）Process Assessment Model v2.5, 2010.（www.automotivespice.com）

ISO/IEC TR 15504-10 に対するセキュリティ拡張の検討

VSE+SS 合同研究会

VSE+SS 合同研究会成果レポートにあるように、「ISO/IEC TR 15504-10（セーフティ拡張）に対するセキュリティ拡張の検討」は、セーフティ／セキュリティのプロセスを通常の開発プロセスに付加するために本合同研究会で検討・定義されたものです。

現在この定義はまだ開発中の版であり、本合同研究会では引き続き早期の完成版の提示に向けて活動を継続します。検討中の事項として、VSE からさらにその先のサプライヤに言及する部分が必要なのかどうかといった点があります。

VSE+SS 合同研究会（以下、本研究会）では、ISO/IEC TR 15504-10（セーフティエクステンション）の内容を参考に、セーフティとセキュリティを融合した対策の検討を行った。

なお、本研究会での研究成果として、本文書の最後にセーフティとセキュリティを融合したモデルの例を示すが、本内容は ISO/IEC TR 15504-10 との直接的な関係を持つものではない。

本研究会では、セーフティとセキュリティを統合した技術を SS（Safety and Security）と呼び、SS を達成するために必要な管理、技術、適格性確認に関するプロセスを以下のとおり検討した。

プロセス群：SSE（Safety and Security Extension）

- SSE.1：SS 管理
  SS 目標を達成するために、ライフサイクル全体を通じて実施すべき SS 活動を計画し、その状況を監視し、逸脱があれば制御するためのプロセス。

- SSE.2：SS 技術
  SS 目標を達成するために、製品に関係するハザードおよび脅威を識別し、それらを回避、抑制するための開発、検証、評価を行うためのプロセス。

- SSE.3：SS 適格性確認
  サプライヤへの開発委託や外部購入など、外部リソースを活用してシステムを開発する場合に、外部リソースを適切に評価するためのプロセス。

これらのプロセスは、ISO/IEC 15504-2 のフレームワークに基づき、ISO/IEC 15504-5 や業界特化版として策定されている Automotive SPICE 等の ISO/IEC 15504 派生モデルへのエクステンションとしても活用が可能である。

プロセス ID	SSE.1
プロセス名	SS 管理
プロセス目的	SS 管理プロセスの目的は、セーフティおよびセキュリティの目標（SS 目標）を満足するために、製品／サービスのライフサイクルを通じて SS 管理活動を確立することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1）SS の原理と基準が確立されている。 2）プロジェクトのための SS 活動の範囲が定義されている。 3）SS 活動が計画され、実施されている。 4）SS 活動を実施するために必要なリソースと作業規模の見積もりが実施されている。 5）SS 管理組織（責任と権限、報告経路、他のプロジェクトまたは組織とのインターフェース）が確立されている。 6）SS 活動が監視され、SS に関する問題が報告され、分析され、解決されている。 7）SS 方針と供給製品またはサービスのための要件の合意が達成されている。 8）サプライヤの SS 活動が監視されている。
基本 プラクティス	**BP1　SS 目標と SS 基準の定義** ハザード／脅威に関する受容可能なリスクの限界が、組織の内外から課された SS 目標または作成された分析／開発方針として定義される。 また、SS 目標かつ／またはリスクの受容可能レベルが定義される。 **BP2　SS ライフサイクルの定義** プロジェクトの目標、SS 基準、状況、複雑性に対して、適切な SS 活動のライフサイクルが定義される。 **BP3　SS 計画の立案** SS 管理と SS 技術の活動は、SS 要求が識別され、それらの依存関係が決定され、それらの実装が計画され、そして、必要なリソースを識別されることを確認し、満足するために実装される。 **BP4　統合された SS 活動の定義** 製品開発、プロジェクトライフサイクル、支援プロセスが統合された SS 活動決定される。 **BP5　スキル要件定義と責任の割り当ての決定** 計画された SS 活動を成し遂げるために必要なスキルが識別され、関連する役割の責任と権限と独立性が定義され、状況に応じて割り当てられる。 **BP6　計画された SS 活動の実装** SS 計画で定義された活動が実装される。 **BP7　SS 活動の展開の監視** SS 活動の展開が監視され、（計画からの）逸脱の是正が実施される。プロジェクトの SS 活動は監視され、作業成果物の SS に関するインシデントが識別され、SS 活動が報告され、分析され、完結さらに中止を管理する。 **BP8　SS 要求と SS 方針の定義とサプライヤとの合意** サプライヤの SS 活動を監視するための方法と技術をサプライヤと合意する。サプライヤから供給された製品の SS を保障する方法の契約を締結する。 **BP9　サプライヤの SS 活動の監視** サプライヤの SS 活動が、SS 要求に合致していることを監視し、報告する。 **BP10　エスカレーションの仕組みの実装** SS 問題を解決するために、適切な管理層への上告が確実に実施されるためのエスカレーションの仕組みが構築され、保守される。

プロセス ID	SSE.2
プロセス名	SS 技術
プロセス目的	SS 技術プロセスの目的は、エンジニアリングプロセスのすべてのステージを通して SS を適切に達成することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1）製品の関係するハザードおよび脅威が識別され分析される。 2）ハザードログが確立され保管される。 3）製品ライフサイクルを通じて SS が確立され、保守される。 4）SS 要求が定義される。 5）SS 統合要求が定義され、配置される。 6）SS 原則が、開発プロセスに適用される。 7）SS の変更要件の影響が分析される。 8）製品が SS 要求に対して検証される。 9）独立した SS の評価が達成される。
基本 プラクティス	BP1　ハザードと脅威の識別 使用条件や予見可能な誤用に関するハザードと脅威が識別される。 BP2　危害とリスクの識別 各ハザード／脅威に対して、（顕在する）可能性、影響の重大さを分析し、ハザード／脅威のリスクを評価する。 BP3　ハザードログの確立と保守 ハザード／脅威への対応のステータスが製品ライフサイクル全体を通して保守される。 BP4　SS の確立と保守 製品ライフサイクル中、段階的に SS を確立し、保守する。プロダクトとプロセス文書が、SS を裏付ける証跡として収集される。 注）SS の裏づけとは、「アイテムが SS 目標を実現しているということを具体的な証跡で明示すること」である。 ISO/IEC15504-1　3.3 項に「アイテムが示す証跡とその依存関係の集合は、リスクが許容される制約内で SS であると正当化すること」であると定義されている。 BP5　SS 要求の確立と保守 ハザード／脅威とリスクの分析結果と他の適用可能な対象に基づいて、製品ライフサイクルを通して SS 要求を確立し、保守する。 BP6　SS 完整性要求の決定 ハザード／脅威のリスク評価に基づき、各 SS 要求に対する SS 完整性要求を決定する。 注）SS 完整性要求とは、「SS 機能が確実に作動するために必要な要件を統合した要求事項のこと」であるつまり、単に SS 要求（SS 機能要求）を満足する SS 機能があるだけでは不十分ということを意味する。 BP7　SS 要求と SS 完全性要求の割り当て SS 要求と SS 完全性要求は、アーキテクチャ、サブシステム、コンポーネントに割り当てられる。 BP8　SS 完全性要求を達成するための SS 原理の適用 要求された SS 完全性要求の達成に関係する原理と方法が、製品ライフサイクル中適用される。 BP9　変更に対する SS 影響分析の実行 ハザード／脅威とリスクの要求変更の影響を分析する。変更要求と、その影響を受ける作業成果物を特定する。 BP10　SS の妥当性確認の実行 ハザード／脅威分析とリスク分析の結果に基づいて、SS 目標が正しく達成されることを確認する。 BP11　独立したアセスメントの実行 要求された独立レベルに従って、製品ライフサイクル期間中のあらかじめ計画された時点で、プロセスと作業成果物に対するアセスメントが実施される。 BP12　市場問題への対策を提供できる体制の構築 製品を市場に供給し続ける間、市場で発生する問題への対策を提供可能な体制を維持する。

プロセス ID	SSE.3
プロセス名	SS 適格性確認
プロセス目的	SS の適格性確認プロセスの目的は、外部リソースを活用して SS に関するソフトウェアまたはシステムを開発する場合に、戦略に従って外部リソースを適切に評価することである。 外部リソースの活用とは、サプライヤへの開発委託、製品に組み込むコンポーネントの購入、開発や管理に用いるツールの購入が該当する。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1）外部リソースを活用するための、SS 適格性確認戦略が作成されている。 2）SS の適格性確認計画が作成され実行されている。 3）SS の適格性確認文書が記述されている。 4）SS の適格性確認報告が提出されている。
基本 プラクティス	**BP1　SS 適格性確認戦略の作成** 適格性確認戦略を作成する。適格性確認戦略は外部リソースに対する品質要求を考慮するべきである。（SS に関係するソフトウェアやシステムに対して SS 要求への影響を決定する。）適格性確認戦略には、達成すべき SS 目標、評価基準、確認結果に基づいた対処方法を含む。 **BP2　外部リソースの完全妥当性確認の計画** 外部リソースに対する SS 適格性確認活動を計画し、各外部リソースに対する適切な適格性確認方法を選択する。 **BP3　外部リソースの適格性確認** 選択された適格性確認方法に従って、適格性確認を実施する。 **BP4　SS 適格性確認結果の記録** SS 適格性確認結果を記録し、利害関係者に通知する。 **BP5　SS 適格性確認結果の更新と保守** 外部リソースを適用した製品／サービスが市場で運用されている期間内は、SS 適格性確認結果とその文書を更新し、保守する。

用語解説

・**セーフティ（安全）**
受容できないリスクがないこと。

・**セキュリティ**
情報の機密性、完全性、可用性を維持すること。

・**ハザード**
人体に危害をもたらす原因となるシステムの故障。

・**脅威**
セキュリティ上のリスクを生じる要因。

・**リスク**
危害の大きさと発生確率の組み合わせ。

・**アイテム**
開発対象

・**サプライヤ**
開発委託先

・**SS 目標**
ハザード、脅威を回避、抑制するために達成すべき目標

・**SS 方針**
ハザード、脅威を回避、抑制するために取るべき活動の方針

・**完整性**
Integrity（インテグリティ）の訳語であり、「完全に整っていること」（JIS X 0160：2012）を意味する。セキュリティの分野ではこの言葉を「完全性」と訳し、「正確さ及び完全さの特性」（JIS Q 27000：2014；情報が破壊されていないことという文脈でつかわれることが多い）といった意味があるが、完整性と訳す場合はそれとはややニュアンスが異なり、要求される事柄が適切な水準で全体として抜かりなく実現されていることを示すことが多い。

VSE セーフティとセキュリティの統合プロセス（VSE-SSE）

ISO/IEC TR 15504-10（セーフティ拡張）に対するセキュリティ再拡張の検討

第１版（2016 年７月７日）

VSE+SS 合同研究会

VSE+SS 合同研究会（以下、本研究会）では、 近年のソフトウェア製品に対するセーフティとセキュリティの必要性の高まりに対して、VSE ソフトウェア開発へのセーフティとセキュリティ拡張の検討を行い、ISO/IEC TR 15504-10（セーフティ拡張）の内容を参考に、以下に示す「セーフティとセキュリティの統合プロセス（SSE：Safety and Security Extension）」を定義した。
なお、このプロセスは、ISO/IEC 15504-2 のフレームワークに基づき、ISO/IEC 15504-5 や業界特化版として策定されている Automotive SPICE 等の ISO/IEC 15504 派生モデルへのエクステンションとしても活用が可能である。

「セーフティとセキュリティの統合プロセス（SS：Safety and Security Extension）」は、「SS 管理」、「SS 技術」、「SS 適格性確認」の３つのサブプロセスから構成される。

プロセス群：SSE（Safety and Security Extension）

・SSE.1：SS 管理
SS 目標を達成するために、ライフサイクル全体を通じて実施すべき SS 活動を計画し、その状況を監視し、逸脱があれば制御するためのプロセス。

・SSE.2：SS 技術
SS 目標を達成するために、製品に関係するハザードおよび脅威を識別し、それらを回避、抑制するための開発、検証、評価を行うためのプロセス。

・SSE.3：SS 適格性確認
サプライヤへの開発委託や外部購入など、外部リソースを活用してシステムを開発する場合に、外部リソースを適切に評価するためのプロセス。

プロセスID	SSE.1
プロセス名	SS管理
プロセス目的	SS管理プロセスの目的は、セーフティおよびセキュリティの目標（SS目標）を満足するために、製品／サービスのライフサイクルを通じてSS管理活動を確立することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）SS達成の原則と基準が確立されている。 ２）プロジェクトのためのSS活動の範囲が定義されている。 ３）SS活動が計画され、実施されている。 ４）SS活動を実施するために必要なリソースが識別され実装されている。 ５）SS管理組織（責任と権限、報告経路、他のプロジェクトまたは組織とのインターフェース）が確立されている。 ６）SS活動が監視され、SSに関する問題が報告され、分析され、解決されている。 ７）SS方針と供給製品またはサービスのための要件の合意が達成されている。
基本プラクティス	**BP1 SS目標とSS基準の定義** ハザード／脅威に関する受容可能なリスクの限界が、組織の内外から課されたSS目標または作成された分析／開発方針として定義される。 また、SS目標かつ／またはリスクの受容可能レベルが定義される。 **BP2 SSライフサイクルの定義** プロジェクトの目標、SS基準、状況、複雑性に照らして適切な、ライフサイクル区分ごとのSS活動が定義される。 **BP3 SS計画の立案** SS要求を満足するためにSS管理とSS技術の活動が識別され、それらの依存関係が決定され、それらの実装計画と、必要なリソースが識別される。 **BP4 統合されたSS活動の定義** SS活動以外の面で見た製品開発、プロジェクトライフサイクル、支援プロセスに統合されたSS活動が決定される。

	BP5 スキル要件定義と責任の割り付けの決定 計画されたSS活動を成し遂げるために必要なスキルが識別され、関連する役割の責任と権限と独立性が定義され、状況に応じて割り付けられる。 **BP6 計画されたSS活動の実装** SS計画で定義された活動が実装される。 **BP7 SS活動の展開の監視** SS活動の展開が監視され、（計画からの）逸脱の是正が実施される。プロジェクトのSS活動は監視され、作業成果物とSS活動上のインシデントが識別され、報告され、分析され、インシデントの完結さらに今後の予防を管理する。 **BP8 SS要求とSS方針についての利害関係者との合意** **利害関係者**間でSS要求とSS実施方針についての合意を確立する。また供給者から供給された製品のSSを確認する方法を合意する。 **BP９ エスカレーションの仕組みの実装** SS問題を解決するために、適切な管理層への上申が確実に実施されるためのエスカレーションの仕組みが構築され、維持される。 **BP10 市場問題への対策を提供できる体制の構築** 市場に供給され、市場での利用／運用によって市場で発生するSS問題への対策を提供可能な体制を維持する。 SS問題への対策を提供する期間および対策の提供方法を定義し、市場に周知する。

プロセスID	SSE.2
プロセス名	SS技術
プロセス目的	SS技術プロセスの目的は、エンジニアリングプロセスのすべてのステージを通してSSを適切に達成することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）製品の関係するSSに関するハザードおよび攻撃者からの脅威が識別され分析される。 ２）ハザードログが確立され保管される。 ３）製品ライフサイクルを通じてSSの論証が確立され、維持される。 ４）SS要求が定義される。 ５）SS完全性要求が定義され、割り付けられる。 ６）SS原則が、製品ライフサイクルに適用される。 ７）SSの変更要件の影響が分析される。 ８）製品がSS要求に対して検証・妥当性確認される。
基本プラクティス	**BP1 ハザードと脅威の識別** SSに関して、システムの使用条件や予見可能な誤用に関するハザードと攻撃者からの脅威が識別される。 **BP2 危害とリスクの識別** 各ハザード／脅威に対して、（顕在する）可能性、影響の重大さを分析し、ハザード／脅威のリスクを評価する。 **BP3 ハザード／イベントログの確立と維持** ハザード／イベントの兆候とそれらへの対応の把握と記録内容の現状が製品ライフサイクル全体を通して維持・分析される。 **BP4 利用状況の変化に対応できるSS要求の妥当性確認** システムの利用条件や利用される環境の変化に対応して、またハザード／脅威の状況の変化に対応してシステムが保守される可能性について、SS要求の妥当性を確認する。 **BP5 SS要求の確立と維持** ハザード／脅威とリスクの分析結果と他の適用すべき事項に基づいて、製品ライフサ

	イクルを通してSS要求を確立し、保守する。 注）「他の適用すべき事項」とは、法的要求、標準、規制、企業方針、顧客要求、顧客及び利用者からのフィードバック、検証結果、品質保証に関わる所見、妥当性確認結果、製造時の経験、設置と撤去時の経験、保守修理の経験、実地運用検討結果などである。 **BP6 SS完全性要求の決定** ハザード／脅威のリスク評価に基づき、各SS要求に対するSS完全性要求を決定する。 注）SS完全性要求とは、「SS機能が確実に作動するために必要な要件を統合した要求事項のこと」である つまり、単にSS要求（SS機能要求）を満足するSS機能があるだけでは不十分ということを意味する。 **BP7 SS要求とSS完全性要求の割り付け** SS要求とSS完全性要求は、アーキテクチャ、サブシステム、コンポーネントおよびサブプロセスに割り付けられる。 **BP8 SS完全性要求を達成するためのSS原則の適用** 要求されたSS完全性要求の達成に関係する原則と方法が一貫して実現されるように、製品ライフサイクル中適用される。 **BP9 変更に対するSS影響分析の実施** ハザード／脅威とリスクの要求変更の影響を分析する。変更要求と、その影響を受ける作業成果物を特定する。 **BP10 SSの検証と妥当性確認の実施** ハザード／脅威分析とリスク分析の結果に基づいて、また、必要なSS活動に特化した検証と妥当性確認を実施して、SS目標が正しく達成されることを確認する。 **BP11 SS活動の論証の論証と維持** 製品ライフサイクル中、SSの論証が確立され、プロダクトとプロセス文書が、SSを裏付ける証跡として収集され維持される。 注）SSの裏づけとは、「アイテムがSS目標を実現しているということを具体的な証跡で明示すること」である。SSの論証とは、たとえば、SSに関するアシュアランスケースやセーフティケースなどである。

プロセスID	SSE.3　（本プロセス項目は、外注・部品ソフト利用・既製品開発環境利用等の外部リソースを活用した開発が行われる場合に適用されるオプション項目である）
プロセス名	SS適格性確認
プロセス目的	SSの適格性確認プロセスの目的は、外部リソースを活用してSSに関するソフトウェアまたはシステムを開発する場合に、戦略に従って外部リソースを適切に評価することである。 外部リソースの活用とは、サプライヤへの開発委託、製品に組み込むコンポーネントの購入、開発や管理に用いるツールの購入が該当する。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）外部リソースを活用するための、SS適格性確認戦略が作成されている。 ２）SSの適格性確認計画が作成され実行されている。 ３）SSの適格性確認文書が記述されている。 ４）SSの適格性確認報告が提出されている。
基本プラクティス	**BP1 SS適格性確認戦略の作成** 適格性確認戦略を作成する。適格性確認戦略は外部リソースに対する品質要求を考慮するべきである。（SSに関係するソフトウェアやシステムに対してSS要求への影響を決定する。）適格性確認戦略には、達成すべきSS目標、評価基準、確認結果に基づいた対処方法を含む。 **BP2 外部リソースの適格性確認の計画** 外部リソースに対するSS適格性確認活動を計画し、各外部リソースに対する適切な適格性確認方法を選択する。 **BP3 外部リソースの適格性確認** 選択された適格性確認方法に従って、適格性確認を実施する。 **BP4 SS適格性確認結果の記録** SS適格性確認結果を記録し、利害関係者に通知する。 **BP5 SS適格性確認結果の更新と維持** 外部リソースを適用し開発された製品／サービスを市場に供給し、市場で発生したSS問題への対策を提供する期間内は、外部リソースを適用し開発された製品／サービスのSS適格性確認結果を維持する。

[用語解説]

・セーフティ（安全）

受容できないリスクがないこと。

・セキュリティ

情報の機密性、完全性、可用性を維持すること。

・ハザード

人体に危害をもたらす原因となるシステムの故障。

・脅威

セキュリティ上のリスクを生じる要因。

・リスク

危害の大きさと発生確率の組み合わせ。

・アイテム

開発対象

・サプライヤ

開発委託先

・SS 目標

ハザード、脅威を回避、抑制するために達成すべき目標

・SS 方針

ハザード、脅威を回避、抑制するために取るべき活動の方針

・完全性

Integrity（インテグリティ）の訳語である。これを完整性と訳す時は、「完全に整っていること」（JIS X 0160:2012)を意味する。要求される事柄が適切な水準で全体として抜かりなく実現されていることを示すことが多い。セキュリティの分野ではこの言葉を「完全性」と訳し、「正確さ及び完全さの特性」（JIS Q 27000:2014; 情報が破壊されていないことという文脈でつかわれることが多い)といった意味がある。完整性と訳す場合とはややニュアンスが異なる。

VSE セーフティとセキュリティの統合プロセス（VSE-SSE）

ISO/IEC TR 15504-10（セーフティ拡張）に対するセキュリティ再拡張の検討

第１版（2016 年７月７日）

VSE+SS 合同研究会

VSE+SS 合同研究会（以下、本研究会）では、 近年のソフトウェア製品に対するセーフティとセキュリティの必要性の高まりに対して、VSE ソフトウェア開発へのセーフティとセキュリティ拡張の検討を行い、ISO/IEC TR 15504-10（セーフティ拡張）の内容を参考に、以下に示す「セーフティとセキュリティの統合プロセス（SSE：Safety and Security Extension）」を定義した。
なお、このプロセスは、ISO/IEC 15504-2 のフレームワークに基づき、ISO/IEC 15504-5 や業界特化版として策定されている Automotive SPICE 等の ISO/IEC 15504 派生モデルへのエクステンションとしても活用が可能である。

■SSE（Safety and Security Extension）

「セーフティとセキュリティの統合プロセス（SSE：Safety and Security Extension）」は、「SS 管理」、「SS 技術」、「SS 適格性確認」の３つのサブプロセスから構成される。

・SSE.1：SS 管理
SS 目標を達成するために、ライフサイクル全体を通じて実施すべき SS 活動を計画し、その状況を監視し、逸脱があれば制御するためのプロセス。

・SSE.2：SS 技術
SS 目標を達成するために、製品に関係するハザードおよび脅威を識別し、それらを回避、抑制するための開発、検証、評価を行うためのプロセス。

・SSE.3：SS 適格性確認
サプライヤへの開発委託や外部購入など、外部リソースを活用してシステムを開発する場合に、外部リソースを適切に評価するためのプロセス。

プロセスID	SSE.1
プロセス名	SS管理
プロセス目的	SS管理プロセスの目的は、セーフティおよびセキュリティの目標（SS目標）を満足するために、製品／サービスのライフサイクルを通じてSS管理活動を確立することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）SS達成の原則と基準が確立されている。 ２）プロジェクトのためのSS活動の範囲が定義されている。 ３）SS活動が計画され、実施されている。 ４）SS活動を実施するために必要なリソースが識別され実装されている。 ５）SS管理組織（責任と権限、報告経路、他のプロジェクトまたは組織とのインターフェース）が確立されている。 ６）SS活動が監視され、SSに関する問題が報告され、分析され、解決されている。 ７）SS方針と供給製品またはサービスのための要件の合意が達成されている。
基本プラクティス	**BP1 SS目標とSS基準の定義** ハザード／脅威に関する受容可能なリスクの限界が、組織の内外から課されたSS目標または作成された分析／開発方針として定義される。 また、SS目標かつ／またはリスクの受容可能レベルが定義される。 **BP2 SSライフサイクルの定義** プロジェクトの目標、SS基準、状況、複雑性に照らして適切な、ライフサイクル区分ごとのSS活動が定義される。 **BP3 SS計画の立案** SS要求を満足するためにSS管理とSS技術の活動が識別され、それらの依存関係が決定され、それらの実装計画と、必要なリソースが識別される。 **BP4 統合されたSS活動の定義** SS活動以外の面で見た製品開発、プロジェクトライフサイクル、支援プロセスに統合されたSS活動が決定される。

	BP5 スキル要件定義と責任の割り付けの決定 計画されたSS活動を成し遂げるために必要なスキルが識別され、関連する役割の責任と権限と独立性が定義され、状況に応じて割り付けられる。 **BP6 計画されたSS活動の実装** SS計画で定義された活動が実装される。 **BP7 SS活動の展開の監視** SS活動の展開が監視され、（計画からの）逸脱の是正が実施される。プロジェクトのSS活動は監視され、作業成果物とSS活動上のインシデントが識別され、報告され、分析され、インシデントの完結さらに今後の予防を管理する。 **BP8 SS要求とSS方針についての利害関係者との合意** **利害関係者**間でSS要求とSS実施方針についての合意を確立する。また供給者から供給された製品のSSを確認する方法を合意する。 **BP９ エスカレーションの仕組みの実装** SS問題を解決するために、適切な管理層への上申が確実に実施されるためのエスカレーションの仕組みが構築され、維持される。 **BP10 市場問題への対策を提供できる体制の構築** 市場に供給され、市場での利用／運用によって市場で発生するSS問題への対策を提供可能な体制を維持する。 SS問題への対策を提供する期間および対策の提供方法を定義し、市場に周知する。

プロセスID	SSE.2
プロセス名	SS技術
プロセス目的	SS技術プロセスの目的は、エンジニアリングプロセスのすべてのステージを通してSSを適切に達成することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）製品の関係するSSに関するハザードおよび攻撃者からの脅威が識別され分析される。 ２）ハザードログが確立され保管される。 ３）製品ライフサイクルを通じてSSの論証が確立され、維持される。 ４）SS要求が定義される。 ５）SS完全性要求が定義され、割り付けられる。 ６）SS原則が、製品ライフサイクルに適用される。 ７）SSの変更要件の影響が分析される。 ８）製品がSS要求に対して検証・妥当性確認される。
基本プラクティス	**BP1 ハザードと脅威の識別** SSに関して、システムの使用条件や予見可能な誤用に関するハザードと攻撃者からの脅威が識別される。 **BP2 危害とリスクの識別** 各ハザード／脅威に対して、（顕在する）可能性、影響の重大さを分析し、ハザード／脅威のリスクを評価する。 **BP3 ハザード／イベントログの確立と維持** ハザード／イベントの兆候とそれらへの対応の把握と記録内容の現状が製品ライフサイクル全体を通して維持・分析される。 **BP4 利用状況の変化に対応できるSS要求の妥当性確認** システムの利用条件や利用される環境の変化に対応して、またハザード／脅威の状況の変化に対応してシステムが保守される可能性について、SS要求の妥当性を確認する。 **BP5 SS要求の確立と維持** ハザード／脅威とリスクの分析結果と他の適用すべき事項に基づいて、製品ライフサ

	イクルを通してSS要求を確立し、保守する。 注）「他の適用すべき事項」とは、法的要求、標準、規制、企業方針、顧客要求、顧客及び利用者からのフィードバック、検証結果、品質保証に関わる所見、妥当性確認結果、製造時の経験、設置と撤去時の経験、保守修理の経験、実地運用検討結果などである。 **BP6 SS完全性要求の決定** ハザード／脅威のリスク評価に基づき、各SS要求に対するSS完全性要求を決定する。 注）SS完全性要求とは、「SS機能が確実に作動するために必要な要件を統合した要求事項のこと」である つまり、単にSS要求（SS機能要求）を満足するSS機能があるだけでは不十分ということを意味する。 **BP7 SS要求とSS完全性要求の割り付け** SS要求とSS完全性要求は、アーキテクチャ、サブシステム、コンポーネントおよびサブプロセスに割り付けられる。 **BP8 SS完全性要求を達成するためのSS原則の適用** 要求されたSS完全性要求の達成に関係する原則と方法が一貫して実現されるように、製品ライフサイクル中適用される。 **BP9 変更に対するSS影響分析の実施** ハザード／脅威とリスクの要求変更の影響を分析する。変更要求と、その影響を受ける作業成果物を特定する。 **BP10 SSの検証と妥当性確認の実施** ハザード／脅威分析とリスク分析の結果に基づいて、また、必要なSS活動に特化した検証と妥当性確認を実施して、SS目標が正しく達成されることを確認する。 **BP11 SS活動の論証の論証と維持** 製品ライフサイクル中、SSの論証が確立され、プロダクトとプロセス文書が、SSを裏付ける証跡として収集され維持される。 注）SSの裏づけとは、「アイテムがSS目標を実現しているということを具体的な証跡で明示すること」である。SSの論証とは、たとえば、SSに関するアシュアランスケースやセーフティケースなどである。

プロセスID	SSE.3　（本プロセス項目は、外注・部品ソフト利用・既製品開発環境利用等の外部リソースを活用した開発が行われる場合に適用されるオプション項目である）
プロセス名	SS適格性確認
プロセス目的	SSの適格性確認プロセスの目的は、外部リソースを活用してSSに関するソフトウェアまたはシステムを開発する場合に、戦略に従って外部リソースを適切に評価することである。 外部リソースの活用とは、サプライヤへの開発委託、製品に組み込むコンポーネントの購入、開発や管理に用いるツールの購入が該当する。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 １）外部リソースを活用するための、SS適格性確認戦略が作成されている。 ２）SSの適格性確認計画が作成され実行されている。 ３）SSの適格性確認文書が記述されている。 ４）SSの適格性確認報告が提出されている。
基本プラクティス	**BP1 SS適格性確認戦略の作成** 適格性確認戦略を作成する。適格性確認戦略は外部リソースに対する品質要求を考慮するべきである。（SSに関係するソフトウェアやシステムに対してSS要求への影響を決定する。）適格性確認戦略には、達成すべきSS目標、評価基準、確認結果に基づいた対処方法を含む。 **BP2 外部リソースの適格性確認の計画** 外部リソースに対するSS適格性確認活動を計画し、各外部リソースに対する適切な適格性確認方法を選択する。 **BP3 外部リソースの適格性確認** 選択された適格性確認方法に従って、適格性確認を実施する。 **BP4 SS適格性確認結果の記録** SS適格性確認結果を記録し、利害関係者に通知する。 **BP5 SS適格性確認結果の更新と維持** 外部リソースを適用し開発された製品／サービスを市場に供給し、市場で発生したSS問題への対策を提供する期間内は、外部リソースを適用し開発された製品／サービスのSS適格性確認結果を維持する。

[用語解説]

・セーフティ（安全）

受容できないリスクがないこと。

・セキュリティ

情報の機密性、完全性、可用性を維持すること。

・ハザード

人体に危害をもたらす原因となるシステムの故障。

・脅威

セキュリティ上のリスクを生じる要因。

・リスク

危害の大きさと発生確率の組み合わせ。

・アイテム

開発対象

・サプライヤ

開発委託先

・SS 目標

ハザード、脅威を回避、抑制するために達成すべき目標

・SS 方針

ハザード、脅威を回避、抑制するために取るべき活動の方針

・完全性

Integrity（インテグリティ）の訳語である。これを完整性と訳す時は、「完全に整っていること」（JIS X 0160:2012)を意味する。要求される事柄が適切な水準で全体として抜かりなく実現されていることを示すことが多い。セキュリティの分野ではこの言葉を「完全性」と訳し、「正確さ及び完全さの特性」（JIS Q 27000:2014; 情報が破壊されていないことという文脈でつかわれることが多い)といった意味がある。完整性と訳す場合とはややニュアンスが異なる。