安全・安心なソフトウェアのためのVSE向けプロセス標準の開発

JISA VSE+SS合同研究会
塩谷和範
伏見愉

ねらい

- 本発表では，VSE（小規模組織）が安全・安心なソフトウェアを開発するための基本的な考え方を手引として提供するとともに、それらをVSEの基本開発プロセスに組み込み活用するためのJISA VSE+SS合同研究会の研究活動と、その成果であるプロセスガイド（手引き）について紹介する。

  - JISA VSE+SS合同研究会†は、JISAのVSE研究会と自動車系安全専門家およびJASA専門家で構成する合同委員会
    - JISA （一社）情報サービス産業協会　VSE普及部会
      Japan Information Technology Service Industry Association
    - JASA（一社）組込みシステム技術協会　安全性向上委員会
      Japan Embedded System Technology Association
  - VSE: Very Small Entity, +SS: + Safety and Security

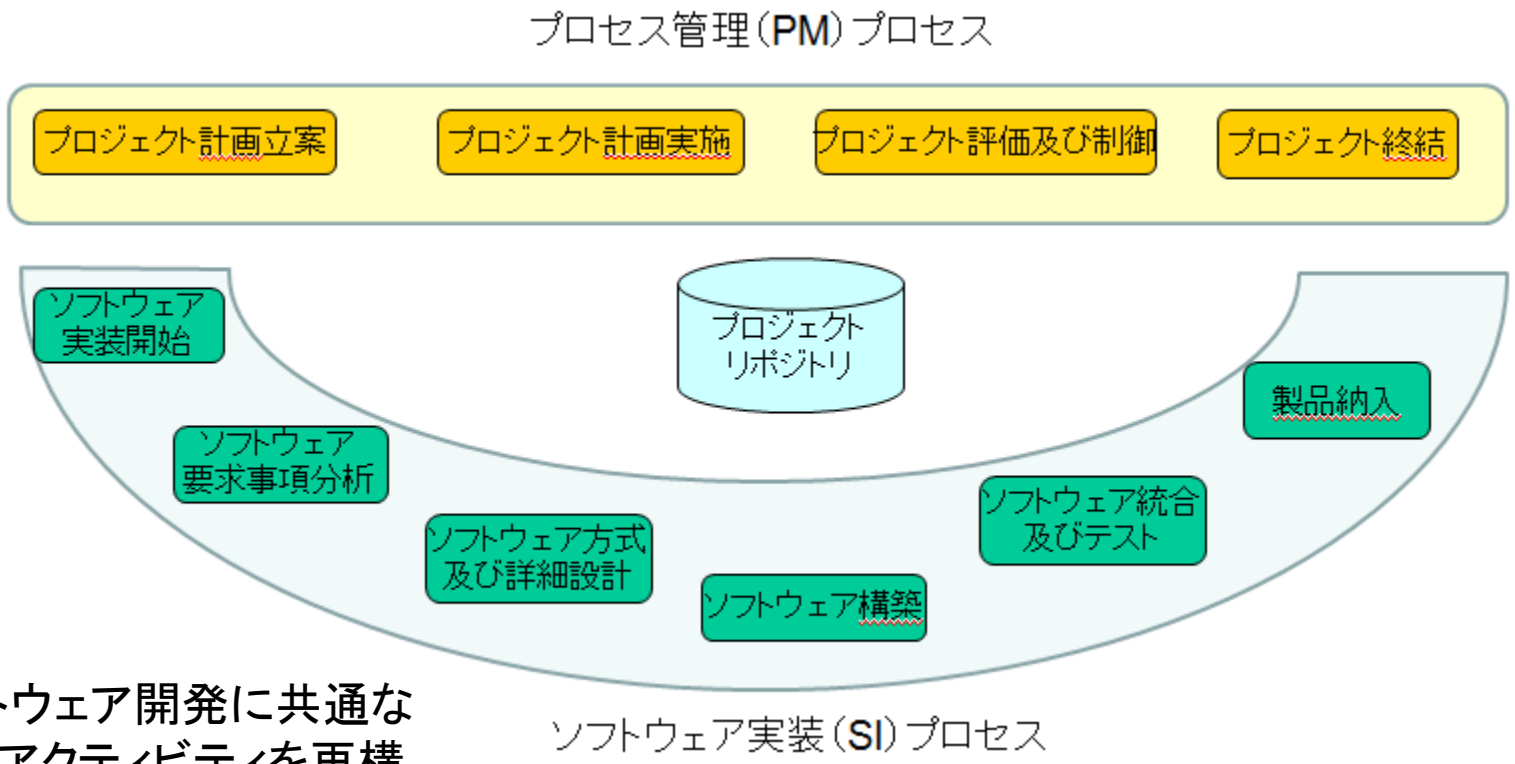
想定する読者・聴衆

- 本研究活動の対象であるガイド（手引き）の想定読者としては、安全(Safety)・安心(Security)に関わるソフトウェアを開発する小規模組織の技術者、プロジェクトマネージャを想定しているが、その他の技術者や管理者にも役立つ情報を提供することを意図している。
  - ここでの安心は、最近大きな問題となってきているソフトウェア製品やサービスなどの安心(Security)を対象とする。

安心・安全拡張の背景(1/2)

- 安全・安心なソフトウェアの開発は、特に組み込み分野や情報サービス分野で、近年ますます切実な課題となってきている。
  - 「つながる世界のセーフティ＆セキュリティ設計入門」SEC BOOKS
- 一方、大企業が提供するシステムおよびソフトウェアの開発の一部を担うのは、中小のソフトウェア企業であることが知られている。
- このような中小規模ソフトウェア開発組織の開発力の底上げのために、ISO/IEC 29110[1]シリーズのプロセス規格、通称VSE規格が2010年に発効している。この規格は、小規模組織(Very Small Entity)向けにソフトウェア開発の基本作業だけに絞り込んで、コンパクトな基本開発プロセスとして再構成した規格で、それ故、リスク管理などを明記せず、特にクリティカルな分野は対象外としている。（図1参照）

VSE規格の基本開発プロセス（図1）



ソフトウェア開発に共通な基本アクティビティを再構成し、関連ドキュメントと関連付け、2つのプロセスにまとめている。

出典: 参考文献[2] VSE標準導入の手引き

VSE規格(ISO/IEC 29110[1])とは

- 小規模組織(VSE)でも実施可能なコンパクトな規格シリーズ
  - 適用しようとする分野で不足する規定や規制があれば適時取り込む
  - 小組織にとっては手に余る規格は使いにくい、規定は最小限とし必要な規定を取り込む方が実際的
  - 対象プロセスの規定に加えドキュメントも提示しわかりやすく実際的
  - アセスメント/認証、システム分野、サービス分野などにも対応
- 対象分野の既存複数規格から、目的に応じて最低限実施しなければならない規定を抜き出し再構成して、プロファイルとしてまとめた仕様とその手引とで構成する。
  - 新たな分野への拡張を現場レベルで行うための日本提案規格がまもなく発行見込み。

    →ISO/IEC TR 29110-2-2 Guide for the development of domain-specific profiles

安心・安全拡張の背景 (2/2)

- VSE規格の開発プロセス導入の手引[2]が2014年に出版されている。しかしながら、小規模組織(VSE)がクリティカルなシステム/ソフトウェア開発の一部を分担している現状では、大企業の製品であっても安全・安心を担保することは難しい。
- そこで、2012年のWOCS2での伏見の発表[3]を受け、VSE規格を拡張して安全・安心についても指針を与え、安全・安心品質の向上を図るための手引きの開発を目指した。
- そのために、JISAのVSE研究WGと自動車系安全専門家およびJASA専門家とで構成する合同研究会†を結成し、業界の実情を反映したコンパクトなVSE向けの安全・安心標準（手引）を開発することにした。

VSEプロセスの安全(Safety)への課題

- 対処すべき課題の第1に、安全(Safety)への考慮がある。
  - VSE（小規模組織）では、個々のメンバの能力（Competency）と組織としての能力との差は大きくはないと考えられるが、本アプローチでは、組織の作業を基本プロセスとして確立し、適切に拡張することにより、組織としての能力を安定させ、向上させることを目指す。

- 既に安全に関するソフトウェアプロセスの国際標準として、ISO/IEC 15504-10[4]が、2011年から提供されているが、これはシステムおよびソフトウェア開発ライフサイクルプロセス全般を規定する通称SLCP[5][6]に、安全についてのプロセスを追加することを前提に提供されている。これをよりコンパクトなVSEの基本プロセスに適応させる必要がある。
  - 注: JIS X 0160:2012 及び共通フレーム2013 (SEC Books) がSLCPに対応

VSEプロセスの安心(Security)への課題

- 第2に安心(Security)に関しては、VSE（小規模組織）などが提供する、システム/ソフトウェア製品の安心に関する国際規格として、ISO/IEC 15408 通称Common Criteria[7]があるが、一部の海外向け製品を除いて日本国内では普及していない。
- また、大掛かりな認証手続きを伴うので大多数のVSEにとっては現実的ではない。従って、VSEでも実施できるやり方を開発する必要がある。
  - 組織の情報セキュリティについてはISMS認証[8]があるが、製品には及ばない。

安全・安心の重要性

- 1　日本における安全意識は高いと思われているが、近年、安全に対する配慮を欠いていると思われる事件・事故が続いている。安全意識の基本を理解し、安全文化を醸成するためにも、簡潔な実際的な指針の普及が望まれる。

- 2　同様に、安心を軽んじたためと思われる事件や抜け穴を狙った侵入事件も相次いでいる。さらに、安心を作りこむべき開発者および安心要求を盛り込む発注者に、受け身ではない安心に対する考え方や取り組み姿勢について、これまでに増して意識させることが、差別化のためにも重要だとの意見がある。

安全・安心拡張のための仕組み

- 3　安全・安心プロセス拡張の仕組みとしては、VSE規格の一部として日本が提案しているVSE規格の拡張法を応用して、VSEの開発基本プロセスに、安全・安心プロセスを追加することで実現できる。

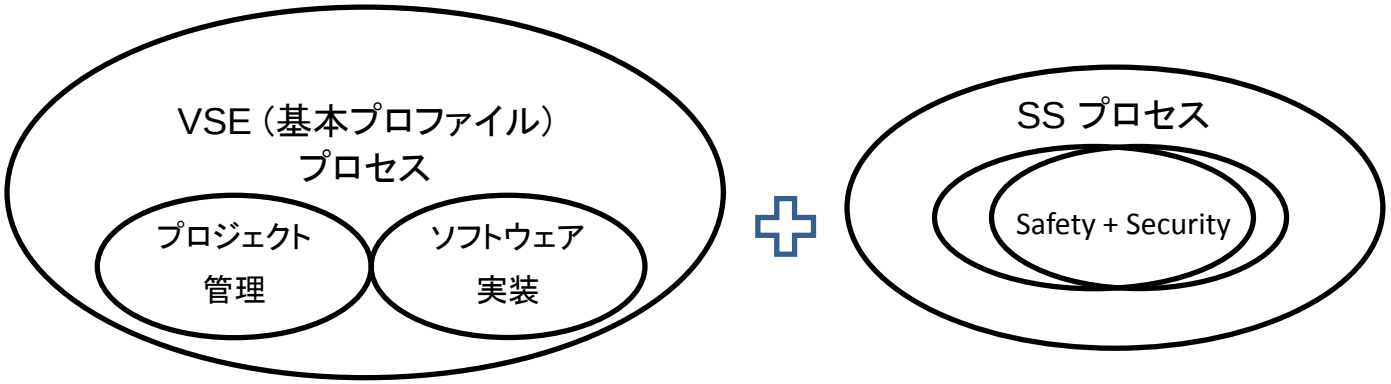


図2　安全・安心プロセスの考え方

安全・安心プロセス拡張方式

- 4　安全プロセス拡張方式としては、先に述べたISO/IEC 15504-10方式が応用できる。また、安心プロセス拡張についても、プロセス拡張の考え方は同じなので、同様のやり方が可能と考える。

- 5　1～4の考察から、安全・安心に関する既存規格や業界ノウハウ、過去事例からの学びなどから安全要件、および安心要件について抽出し、VSEの基本プロセスに対応させたISO/IEC 15504-10方式の拡張による、安全・安心プロセス拡張を実現することにした。

  – 検討の結果、プロセス視点でほぼ同一に規定できることが分かった。

SSプロセスガイド (Safety and Security Extension)

- セーフティとセキュリティとを統合した技術を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拡張プロセスを定義する。
- プロセス群：SSE（Safety and Security Extension）
  - SSE.1：SS管理
  - SSE.2：SS技術
  - SSE.3：SS適格性確認
- このSS拡張をVSEで活用するために、ISO/IEC 15504-2に定義されたPA 2.1およびPA 2.2の達成成果に、SSについての追加拡張を行うことを検討している。
  - VSEでも実施できるように規定し過ぎない。

開発者向けの簡潔な要点解説(実施指針)

- セーフティの基礎
  - ISO 26262等の推進や現場実施に必要な原則的な観点の解説
  - リスクのとらえ方のポイント
  - ガイド類の間違った使い方に対する実務的な要注意点

- セキュリティの基礎
  - 製品のセキュリティ理解に必要な原則的な観点の解説
  - リスクのとらえ方のポイント
  - 開発プロセスの中でのセキュリティ実装の手法・ツールやガイドの紹介
  - セキュリティ事故例と開発者の留意点

VSE規格の安全・安心拡張の成果物

VSE標準 (ISO/IEC 29110) と「VSE標準導入の手引」と合わせて利用する、
■ 開発現場での深い理解に基づくプロセスの確立・実施のために、報告書及び、実施指針として「セーフティの基礎」と「セキュリティーの基礎」を公開
■ VSE標準プロセスに追加する安全・安心プロセス拡張ガイドを公開

VSE標準
導入の手引

SSプロセス
ガイド

合同研究会
成果報告書

セーフティ
の基礎

セキュリティ
の基礎

■ガイドラインとしての利用
■アセスメントのプロセス参照モデルとしての利用
■その他、発注条件や認証としての利用

VSE規格の安全・安心拡張の期待効果

- VSE規格の基本プロセスとその安全・安心プロセス拡張は、自己診断やアセスメントの際の参照モデルとして活用できる。現在VSE向けのアセスメント規格が審議中であるが、従来のISO/IEC 15504（通称SPICE）アセスメントを使ってもよい。また、受発注の際の成果物の確認に使うこともできる。さらに、現在審議中の認証規格を実施する環境が整った際には、VSE認証を取得することも可能となる。
  - いわゆるISO認証は、ISOが実施し認定するものではなく、該当ISO規格に適合しているかを、第一者、第二者、第三者がISO/IEC 17000による適合性評価を行うものである。（ISO/IEC Directives Part 2 の 6.7）
  - VSE認証は、VSE規格への適合性を認証することを想定している。

まとめ(今後の課題)

- VSE+SS合同研究会での成果は、コンパクトな扱いやすいものであり、それぞれの開発現場でのニーズに合わせた開発プロセスの拡張に利用し、目的とする成果物の安全・安心の向上に役立つものと考える。また、これを活用することで、製品品質の向上および組織の競争力向上により、ビジネス上の信用を勝ち取ることに役立つものと考える。
- 今後の課題としては、今回の手引きの作成をもととして、より充実した手引きやツールを提供すること、およびワークショップやセミナーなどの開催を通じて、VSEの安全・安心文化の普及を図りたいと考えている。また各開発組織において手引きを生かしたより具体的な状況に応じたプロセスガイドが開発されることが期待される。

補足：CompetencyとSkillについて

- 技術者個々のスキルや能力は、ソフトウェア開発組織の開発力の根幹をなす。そのため、VSE基本プロセスとその安全・安心プロセス拡張への取り組みとは別に、ETSS/ITSS (SEC Books)などを活用した人材育成が組織の対応として求められる。
  - Functional Safety (IEC 61508)分野の専門家とチームのCompetencyは、COMPETENCE MODEL に基づきアセスメントのやり方まで規定した次のガイドがある。
    - Competence Criteria for Safety-related system practitioners, Guidance provided by the IET

- 「組込み開発ガイドESxRシリーズ」(SEC Books)には、ドキュメント例が含まれており参考になる。

用語・文献

用語はJISを基本とした。参考文献を次に示す。（対応JISを併記する。）

[1] ISO/IEC 29110 Systems and Software Engineering — Lifecycle Profiles for Very Small Entities (VSEs)
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45086.
JISX0165-2 小規模組織のソフトウェアライフサイクルプロファイル－第2部：枠組み及び分類指針

[2] VSE標準導入の手引き JISA 標準化部会 VSE標準普及WG,
http://www.jisa.or.jp/publication/tabid/272/pdid/VSE2014/Default.aspx,

[3] 「小規模組織（VSE)プロセス規格はクリティカルソフトウェアにどう活用できるか（チュートリアルとして）」
伏見　諭, www.ipa.go.jp/files/000004109.pdf, http://stage.tksc.jaxa.jp/jedi/event/20120927.html

[4] ISO/IEC TS 15504-10:2011 Information technology — Process assessment — Part 10: Safety extension
JISX0145-2 情報技術－プロセスアセスメント－第2部：アセスメントの実施　(Part10は未訳)

[5] ISO/IEC 12207 Systems and software engineering — Software life cycle processes
JISX0160 ソフトウェアライフサイクルプロセス

[6] ISO/IEC 15288 Systems and software engineering — System life cycle processes
JISX0170 システムライフサイクルプロセス

[7] ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
JISX5070-1 セキュリティ技術－情報技術セキュリティの評価基準－第1部：総則及び一般モデル

[8] ISO/IEC 27001:2013 Information technology - Security techniques-Information security management systems-Requirements
JIS Q 27001:2014 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項

Q&A

ご静聴ありがとうございました。
ご意見、ご質問を承りたいと思います。

よろしくお願い致します。

kazshioya@gmail.com
satoshi.fushimi@sofdela.info