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

塩谷和範† 伏見愉†

A process standard for developing Safety and Secure software

SHIOYA Kazunori, FUSHIMI Satoshi

ねらい 本稿では，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。

キーワード VSE，小規模組織，29110 標準，安全，安心，+SS

Target: *This abstract is to provide criteria and advice for the purpose of better understanding of your 13thWOCS[2] abstract in audience and reviewer.*

Keywords: VSE, Very Small Entity, 29110 standard, safety, security, +SS

1．想定する読者・聴衆

本稿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。

2. 安心・安全拡張の背景

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。

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）

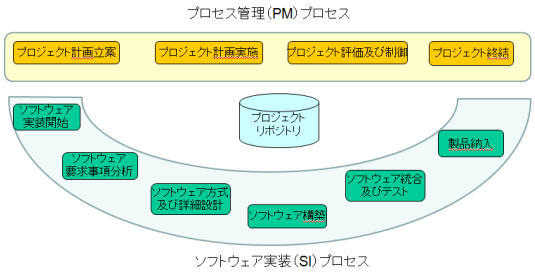

図 1 VSE プロセスとアクティビティ

しかしながら、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[2]の発表を受け、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すことにした。

そこで、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†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・安心の手引を作成することにした。

3. VSE プロセスの安全・安心への課題

対処すべき課題の第 1 に、安全(Safety)への考慮がある。

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[3]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[4][5]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

†JISA VSE+SS 合同研究会 (VSE + SS joint study group)
Japan Information Technology Service Industry Association, 9th Fl, Nittobo Bldg, 2-8-1 Yaesu, Chuo-ku, Tokyo 104-0028, Japan
E-mail: kazshioya@gmail.com, satoshi.fushimi@sofdela.info

されている。これをよりコンパクトな VSE の基本プロセスに対応させる必要がある。

第 2 に安心(Security)に関しては、VSE 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、Common Criteria[6]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。

4. VSE 規格の安全・安心拡張のための方策

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書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、安心の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。

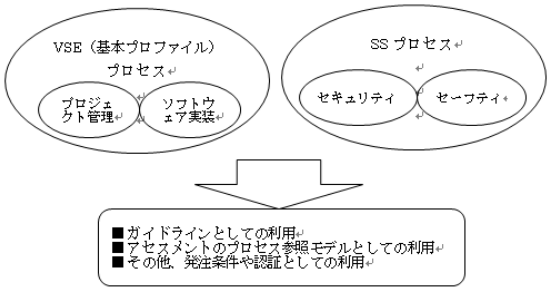

図 2 VSE+SS の考え方

3　安全・安心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、安全・安心プロセス拡張を実施することができる。（図 2 参照）

4　安全拡張方式としては、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　以上の考察から、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 方式拡張による、安全・安心拡張を実現することにした。

5. VSE 規格の安全・安心拡張の期待効果

VSE 基本プロセスとその安全・安心拡張プロセスは、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。

6. まとめ(今後の課題)

VSE+SS 合同研究会での成果は、軽量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。

7. 用語・文献

用語については JIS を基本とした。略語および文献は次に示す

文　　献

[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.

[2] 「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

[3] ISO/IEC TS 15504-10:2011 Information technology — Process assessment — Part 10: Safety extension

[4] ISO/IEC 12207 Systems and software engineering — Software life cycle processes

[5] ISO/IEC 15288 Systems and software engineering — System life cycle processes

略 号 一 覧

VSE: Very Small Entity.
+SS: + Safety and Security.
JISA: Japan Information Technology Service Industry Association
JASA: Japan Embedded System Technology Association.

付録　なし