# 「ソフトウェア品質向上・保証に関する取り組み」

渡辺弘美@JETRO/IPA NY

## １．米国におけるソフトウェア危機

米国はソフトウェア開発に関して世界の最先端を誇っている一方、最近ソフトウェアの信頼性をめぐる問題がクローズアップされ、連邦政府や業界の間で、ソフトウェア品質を改善するための方策が議論されている。ソフトウェアのバグによる莫大な経済コストのみならず、最近ではソフトウェアの不具合による人身事故も報道され、ソフトウェアの低品質は社会問題化している。さらに米国ソフトウェアの品質が国際的にみてもレベルが低いという電気電子技術者協会（IEEE）の調査結果が出され、米国ソフトウェア業界の優位性は揺るいでいる。この報告書によると、プログラムの 10 万ラインに含まれる不具合率測定調査によれば、日本が２ポイントと圧倒的に低いのに比べ、欧州他が 24、インドが 26 であったのに対して、米国は 40 と非常に不具合率が高いことが判明している。米国ではソフトウェア産業の国際競争力の観点からも、IT 分野で国際的リーダーの座を明け渡すことはしまいと、“ソフトウェア危機”問題に取り組む姿勢が活発化している。

### (1)　経済的損失

ソフトウェア信頼性に対する議論を高める火付け役になったのは、2002 年 5 月に商務省技術標準局（NIST）が発表した『The Economic Impact of Inadequate Infrastructure for Software Testing』という報告書である。NIST はリサーチ・トライアングル研究所（ノース・カロライナ州）との共同調査の結果、ソフトウェアの品質が悪いために、米国経済は全体で年間 595 億ドルの損害を被っており、そのうち約 3 分の 1（222 億ドル）は、最適な検証が行われていれば問題回避できたはずであると断言した。

不適当なソフトウェア検証によって生じた経済コスト

| コスト負担者 | 不適当なソフトウェア検査によって生じたコスト（億ドル） | 検査を改善すれば削減可能なコスト（億ドル） |
|---|---|---|
| ソフトウェア開発者 | 212 | 106 |
| ソフトウェア・ユーザ | 383 | 117 |
| 計 | 595 | 222 |

同調査では、不適当なソフトウェア検査によって生じたコストのうち、ユーザがソフトウェアの欠陥を修復するのにかける割合についても試算し、その総額が年間 383 億ドルに達すると報告している。これは先にあげた年間損失額の約 6 割を、ユーザが負担している計算になる。ソフトウェアの品質問題は、ユーザや最

終製品に近くなるほどその修正費は巨額に膨れ上がる。例えば、交換機や航空機などの高度なシステムの場合、導入後のバグ修正コストは数億ドルを下らないといわれている。

ソフトウェア完成後のバグに関する調査は *Information Week* 誌でも行われた。同誌が 2002 年にＩＴ関連マネージャー800 名を対象に調査を行ったところ、回答者のうち 97 パーセントがソフトウェアのバグによる問題が発生したと答え、その中の約９割が、コストが非常に高くついたり、収入を失ったりといった経済的損失を被ったとしている。また回答者の 60 パーセント以上が「ソフトウェア会社はバグなしソフトウェアを作るための努力が足りない」と考えていることが明らかになっている。

また、米国においては、最近、ソフトウェア不具合で以下のような大きな経済的損失をもたらした事件が起きた。

ソフトウェア不具合による主な経済的損失事件

| 時期 | 事故の概要 |
|---|---|
| 2004 年 8 月 | American Airline と US Airway の燃料管理、操縦士やフライトアテンダントのスケジュール調整、機内食管理などを行う出発前フライト・オペレーション・データベース・システムが故障。American Airline と US Airway であわせて約 350 以上のフライトがキャンセル又は遅れが出て、数千人の搭乗客に影響が出た。両航空会社に対する乗客の不満が噴出し、ブランド・イメージに傷をつけた。（被害を受けた乗客の訴訟の動きは現在未定。） |
| 2004 年 5 月 | ダイムラー･クライスラーのメルセデス･ベンツの電子制御ブレーキシステム『センソトロニック』について、油圧ブレーキのコントロールユニットのプログラムに不備が見つかり、68 万台をリコールの対象とした。同社としては最大規模のリコール台数。 |
| 2001 年 6 月 | ニューヨーク株式相場がソフトウェア不具合によりダウンし、90 分間取引を停止させた。システム復旧後も、取引は低調であった。 |
| 2000 年 10 月 | ロスアンゼルス空港管制センターのシステムに不具合があり、カリフォルニア州、ネバダ州、アリゾナ州、ユタ州などの一部地域で 4 時間にわたり離陸できなくなった。 |
| 1999 年 6 月 | オンライン・オークション・サイトの eBay が 22 時間ダウンし、単に売上に影響を及ぼしただけでなく、株式市場の時価総額で 57 億ドル失った。 |
| 1999 年 | NASA の火星探査機はソフトウェア不具合によりエンジン故障が発生。これにより 3 億 6 千万ドルの探査機は破壊されてしまった。 |

## (2)　ソフトウェアの不具合による死傷事故

こうした経済的損失に加え、ソフトウェアの不具合が原因で死傷者を出す惨事も引き起こしている。最近米国で起きた死亡事故に発展した主な事件には以下のものがある。

ソフトウェアの不具合による主な死傷事故

| 年 | 死者（人） | 事故の概要 |
|---|---|---|
| 2003 | 3 | ソフトウェアの不具合により、北米とカナダの一部で停電が発生。 |
| 2001 | 5 | パナマの病院で、癌治療に利用する放射線装置のソフトウェアにミスがあり、患者に対して許容以上の放射線を浴びせた。 |
| 2000 | 4 | 海兵隊垂直離着陸機（Osprey）の墜落事故はソフトウェアの『奇形』が原因とされている。 |
| 1997 | 225 | レーダーにソフトウェアの欠陥があったため、韓国航空機の墜落を防げなかった。 |
| 1997 | 1 | ソフトウェアの論理エラーによって、薬物注入ポンプが患者に致死量を超えるモルヒネ硫酸塩を注入。Gish Biomedical 社は同装置のソフトウェアを再度プログラミングし直した。 |
| 1995 | 159 | コロンビア共和国のカリ市に向かって降下していた American Airlines のジェット機が山中で墜落。陪審員はこの事故の責任の 17%はフライト管理システムのメーカーにあるとの判決を下した。コロンビアの Aeronautical Civil が発表したレポートによれば、同システムのソフトウェアがパイロットに不十分でかつ矛盾する情報を提供し、パイロットに方向を誤らせたとしている。 |
| 1991 | 28 | ソフトウェア不具合のために、パトリオット・ミサイルの集中砲火によってイラクのスカッド・ミサイルを打ち落とすことができず、サウジアラビアにあった米軍兵舎がスカッド・ミサイルの攻撃を受けた。 |
| 1985 | 3 | ソフトウェア設計上のミスにより、放射線医療装置 Therac-25 がアメリカ人とカナダ人の患者に、許容量以上の放射線を浴びさせた。 |

死傷事故に直結するケースとして医療システムのソフトウェア不具合が最近重要な問題になっている。上記 8 件の主だった事件の中でも 3 件（1985 年、1997 年、2003 年）が医療機器のソフトウェア不具合によるものである。このほか、2002 年に食料医薬品局（FDA）が行った調査によれば、1992 年から 1998 年に、3140 件の医療機器リコールが報告され、そのうち、7.7 パーセントに当たる 242 のリコールはソフトウェアの不具合が原因としている。しかし、242 件以外のケースの中には問題の原因がソフトにあるのかハードにあるのか明確でないものも含まれているため、ソフトウェア不具合を原因とするリコールの数字はさらに大きいと見ている。死亡事故に至らなかったものの、そうした事故を引き起こす可能性のある医療システムが市場に出回っている実態が深刻であることを示している。

## ２．ソフトウェア品質向上に向けた米国政府の取り組み

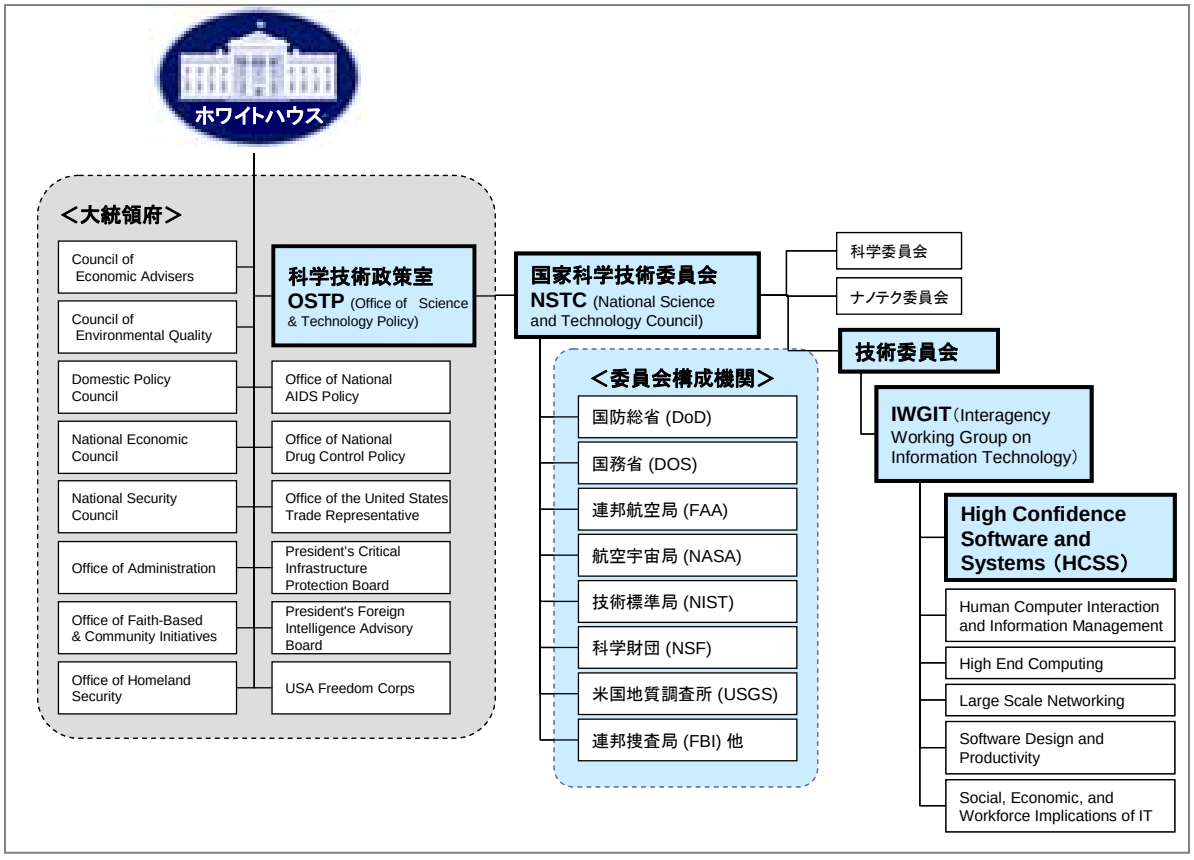
ソフトウェアの品質が悪いために経済的損失や死傷事故が引き続き起こっている現状に鑑み、このような問題を解決するために米国では国家レベルで取り組み

を行っている。その旗振り役として、米国政府は関連機関を横断的に統括し政策を議論できる仕組みを活用している。

(1)　High Confidence Software and Systems (HCSS)

米国連邦政府におけるソフトウェア品質向上の取り組みは、ホワイトハウスの下部組織である「高信頼ソフトウェア・システムズ＝HCSS（High Confidence Software and Systems）」というワーキング・グループを中心に行われている。大統領府の１つである科学技術政策室（OSTP）の管理下に置かれる国家科学技術委員会（NSTC） 技術委員会の省庁間横断ワーキング・グループの１つとして位置づけられている。

ホワイトハウス大統領府における HCSS の位置づけ




①HCSS 設立経緯と目的

HCSS（発足当時の名称は High Confidence Systems）は 1998 年、新たな連邦政府の IT 研究開発活動の１つとして発足した。きっかけとなったのは、1995 年と 1997 年に開催された国家科学技術委員会（NSTC）の「コンピューティング・情報・コミュニケーションに関する委員会＝CCIC（Committee on Computing, Information, and Communications) 」によるワークショップの中でソフトウェアの信頼性（ハイコンフィデンス・コンピューティング）に関する議論がクローズア

ップされたことに端を発している。1998 年に省庁間横断のワーキング・グループが発足され、2010 年の研究完了を目標として活動が展開されている。

HCSS が目指すのは、ソフトウェアの能力を高めるだけでなく、その信頼性、安全性を向上させ、ソフトウェアの長期利用やシステム修復能力を可能にする技術の研究開発を行うことによって、ミッション・クリティカルなシステムの品質を向上させることである。HCSS は設立アジェンダの中で「国民を守り、消費者を守り、政府のサービスを向上させる（Protect the Public, Protect the Consumer, & Enhance Government Services）」ことを究極的な目的として掲げている。

②HCSS の活動に関連する政府機関

HCSS には設立当初から様々な政府機関が関係してきたが、特に近年、活発に参加している機関としては、国防総省国防高等研究事業局（DARPA）、科学財団（NSF）、航空宇宙局（NASA）、国家安全保障局（NSA）、国立標準技術研究所 （NIST）、連邦航空局（FAA）、FDA、国防総省（DOD）関連機関などがある。

③主な活動内容

これまでの主な活動としては、高い信頼性を求められるシステム構築に関する研究・開発プログラムの推進やワークショップ開催などが含まれている。

例えば、研究・開発の推進活動としては NSF と NASA が中心となって行っている「Highly Dependable Computing and Communication Systems Research (HDCCSR)」 という研究プログラムがある。HDCCSR では、NSF のグラントを獲得した研究者が研究の成果を、実際の NASA の研究所（カリフォルニア州の Ames Research Park）で実証試験を行うことによって、その理論の現場での有用性を検証することを目的としている。最終的にはソフトウェア・ベースのシステムの信頼性を数量的に測定し、予測できるようにするための基礎を築こうと試みている。

一方、ワークショップとしては、特に航空・医療関係のシステムに関するものが多く、Critical Aviation Systems Workshop (2000)、High Confidence Aviation Systems (2000)、Medical Devices Software Safety Workshop (2000) などがある。

④HCSS の議論の深化

このように政府関係機関中心で進められていた HCSS における活動は、2003 年度から大学の研究者を取り込んだ方向性へ展開をみせ、現在 National Academies of Sciences の中に設置された CSTB（Computer Science and Technology Board）の特別委員会（Sufficient Evidence　Building Certifiably Dependable Systems）で突っ込んだ議論が進められている。中心的なメンバーには、マサチ

ューセッツ工科大学、カーネギーメロン大学等の教授陣に加え、Sun Microsystems や Microsoft など民間企業の研究者らが参加している。

同委員会は HSCC の議論を２つのフェーズを設けている。第１フェーズは、現状のソフトウェア保証制度における問題点と必要性を認識するためのワークショップを開催し、これからの研究課題について整理を行うというものである。第２フェーズは、第１フェーズを元に大学・企業などから研究成果を集め、最終報告をまとめる計画になっている。現在は第１フェーズのワークショップが進行中である。

⑤CSTB の特別委員会における議論のポイント

同特別委員会では、４つの点に焦点を当てている。第１のポイントは、CMM や ISO9000 といった既存のソフトウェア・プロセス評価を見直す動きである。ソフトウェア開発プロセスのレベルが高いことが、ソフトウェアそのものの高品質と結びついていないのではないかという疑念が関係者の間で高まっている。しかし、この問題意識に対して、ソフトウェアそのものの品質をいかに評価すべきかという代替案は出てきていないというのが現状で、技術的解決策を模索する必要性が強調されている。

第２に、ソフトウェアの品質保証は企業経営や法律問題に絡む問題であるという点を指摘している。例えば、１つのシステム開発に非常に多くの関係者が絡んでいるために、責任の所在を明らかにするために、保証制度の必要性がこれまで以上に高まってきているという点が指摘している。その一方で、保証制度を多くのシステムに要求すると、時間・費用といったコストがかさみ、商品の競争力が落ちるという問題が産業界から指摘されており、現実的な保証制度の構築が迫られている。

第３に、政府機関での民生用（COTS＝commercial-off-the-shelf）ソフトウェアの導入が増えることによって、システム及びデータの信頼性が低下するのではという懸念が挙げられている。現在、米政府はコスト削減のため COTS 利用を促進している。この流れは、システム運用の危険性が高く、データの秘匿性が強く求められる航空や軍事関連のシステムにまで広がっている。独自システム開発の場合と異なり、COTS 利用では、政府がシステム開発プロセスへ関与することが難しい。そのため COTS 利用に向けた対策が求められている。

そして第４に、ソフトウェアの信頼性を向上させるため、ソフトウェア・ライフサイクルの各フェーズに応じた品質改善技術の研究・開発を促進することの重要性が指摘されている。

(2)　国防総省(DOD)を中心としたプロジェクト

連邦省庁の中でも DOD はホームランド・セキュリティという観点から他の関係政府機関を取り込んだソフトウェア品質向上の取り組みを行っている。

2002 年 10 月、「基幹インフラストラクチャ保護に関する大統領諮問委員会＝PCIPB（President's Critical Infrastructure Protection Board）」は、ITSSG（IT Security Study Group）を結成し、既存のソフトウェア品質保証制度に関するレビューを行った。その結果を元に、DOD 関連機関は、既存保証制度の改善策の検討を開始。翌年 10 月には、ソフトウェア品質保証専門のポジション（Deputy Director for Software Assurance）を設置し「ソフトウェア品質保証プログラム（Software Assurance Program）」を立ち上げている。

「ソフトウェア品質保証プログラム」には５つのワーキング・グループが含まれている。

- WG1: Security Process Capability Evaluation
- WG2: Software Product Evaluation
- WG3: Counter Intelligence Support
- WG4: Acquisition/Procurement and Industrial Security
- WG5: User Identification of Protected Assets

DOD は「ソフトウェア品質保証プログラム」を発足させる以前の 2002 年５月から、FAA と協同主催で、CMMI を拡張し、ソフトウェア品質を向上させるためのワーキング・グループを開催している。このグループには、NASA、DOE といった米連邦政府機関のみならず、英国防省、オーストラリア国防省の DMO（Defense Material Organization）や関連産業が参加している。

## ３．他の連邦政府省庁におけるソフトウェア品質保証制度

米連邦政府はソフトウェアの欠陥によって生じる損害を減らすため、ソフトウェアの品質保証制度を導入してきた。特に、人命に関わる機器を提供する産業（医療、航空、核エネルギーなど）に対して、監督官庁はそれぞれ独自のソフトウェア保証基準を満たすことを義務付けてきた。また、個人情報の保護と信頼性の高いデータが求められる電子投票システムについても高いソフトウェア品質が求められるため保証制度が採用されている。

主要政府機関のソフトウェア保証制度の概要

| | 管轄政府機関 | 対象システム | 法規・ガイドライン | 検証対象 | 認定機関 |
|---|---|---|---|---|---|
| （１） | 連邦航空局（FAA） | 航空機搭載システム | 国際協定 DO-１７８B | 航空機メーカー | 外部認定専門家・企業：Designated Engineering Representatives (DER) |
| （２） | 食品医薬局（FDA） | 医療機器システム | Premarket Notification of the Food, Drug and Cosmetic 法 510 (k) 条 | 医療機器メーカー | FDA 内部機関：Office of Device Evaluation (ODE) |

| | | | | | |
|---|---|---|---|---|---|
| （３） | National Association of State Election Directors （NASED） | e-Voting (電子投票)システム | Federal Voting Systems Standards | IT ベンダー | 外部委託機関：Independent Testing Authority (ITA) |

(1)　連邦航空局（FAA）

①背景

FAA は国際航空交通管理協定（Global Aviation Traffic Management Agreement）に基づき、民用・軍用の全ての航空機搭載システムについて、DO-178B（Software Considerations in Airborne Systems and Equipment Certification）という品質保証を取得するよう各ベンダーに求めてきた。ベンダーは新規システムに限らず、改良システムについても DO-178B の保証検査対象としている。第 1 版は 1982 年に RTCA（Radio Technical Commission for Aeronautics）によって作成され、最新版は 1992 年に発表されている。

②制度の概要

FAAのソフトウェア品質保証検査はDER（Designated Engineering Representatives）と呼ばれるFAA外部の専門家が行っている。DERとは、連邦規則集 14（Aeronautics and Space）の 183.29 条の規定によってFAAが認定する品質検査官である。ソフトウェア品質管理のほかに、無線、エンジン、プロペラ、動力装置を含む９つの航空機関連の品質チェックを行う際に導入されている。DER にはエンジニアリングの学位、もしくはそれに相当する知識や経験を持つ個人がコンサルタントとして認定される場合（Consultant DER）と、そうした人材を抱える企業が認定される場合（Company DER）の二つのタイプがある。DERの詳細な認定基準はFAA Order 8100.8 によって定められている。ソフトウェア品質検査を行うDERは、DO-178Bに基づき審査を行う。

DO-178B の審査では、ソフトウェア開発プロセス検査、ソフトウェア・ライフ・サイクルごとに生じた問題分析、ソフトウェア機能検査（要求水準の達成度と堅牢度の両者）、プログラム・コーディング内容の検査の４つが行われる。DO-178B では、検査対象とするシステム不具合によって起こる危険度に応じて、５つのシステム要求水準を規定している。

- Level A：　ソフトウェアにミスがあった場合、大惨事となる。
- Level B：　ソフトウェアにミスがあった場合、大きな被害が発生する。
- Level C：　ソフトウェアにミスがあると、被害が起きる。
- Level D：　ソフトウェアにミスがあっても小さな問題しか起きない。
- Level E：　ソフトウェアにミスがあっても問題は起きない。

③現行制度の課題・問題点

2002 年に開かれたFAAのNational Software Conferenceの『DO-178B – A Square Peg in a Round Hole?』というセッションの中で、DO-178Bの適用で安全性が高まっているかどうか数値的根拠に欠け、現行システムが安全性を保証するものとして継続して利用するに値するものなのかといった点に関して検討が必要とされている。また、現行制度では、「how unsafe a system is when it fails（ソフトウェアに不具合があった場合、どんな危険が待ち構えているか）」に終始し、「how safe a system is when it is working (システムが機能すると、どれほど安全なものなのか)」という前向きなアプローチをとっていないという指摘もなされている。FAAとRTCAは次期バージョンDO-178Cにこうした課題を盛り込むことが必要となっている。

(2)　食料医薬品局（FDA）

①背景

FDA では、食品・医薬品・化粧品の市販前届出に関する法律（Premarket Notification of the Food, Drug and Cosmetic 法 ）の 510 (k) 条の中で、医療機器に関しては、市場に提供する少なくとも 90 日前までに、FDA に対して機器の登録を行うことを義務付けられている。 FDA は医療機器のソフトウェア品質のガイドライン作成に 1986 年から取り組んできた。1987 年には、FDA の下部組織である Center for Devices and Radiological Health（CDRH）の Office of Device Evaluation (ODE) がコンピューター・ソフトウェア関連医療機器の『市販前レビュー（Premarket Review）』を実施するための特別委員会を結成し、1998 年に『Reviewer Guidance for Computer Controlled Medical Devices』のドラフトを作成。従来から医薬品などの市場投入前検査を義務付けてきた 510(k) にソフトウェアの項目を設けるというもので、その後、産業界などの関係団体の意見等を取り込み、1991 年にガイダンスが発表された。それ以降、アップデートがされ、最新版『Guidance for FDA Reviewers and Industry: Guidance form the Content of Premarket Submissions for Software Contained in Medical Devices』は 1998 年に発表されている。

②制度の概要

審査は ODE が 510(k)に基づいて審査を行う。510(k) では、システム要求水準を以下の３レベルに分けており、レベルに応じて要求されるドキュメントの量及び報告内容が増え、より詳細で厳格な審査が行われる仕組みとなっている。

- Major ：ソフトウェアの不具合によって、患者もしくは操作担当者が重度の傷害を受けるもしくは死に至る。

- Moderate：ソフトウェアの不具合によって、患者もしくは操作担当者が軽度の傷害を受ける。
- Minor：ソフトウェアの不具合があっても、特に人間に害を与えることはない。

各レベルごとに求められるドキュメント検査の概要

| ガイダンスの条項 | 検査対象 | レベル | | |
|---|---|---|---|---|
| | | Minor | Moderate | Major |
| 2, 3.1 | 医療機器の利用目的に応じたシステム要求水準レベル | ○ | ○ | ○ |
| 3.2 | ソフトウェア・システム説明 | ○ | ○ | ○ |
| 3.3, 3.4 | 対象機器の危険性分析 | ○ | ○ | ○ |
| 3.4, 4.2 | ソフトウェア・システム仕様書 | ○ | ○ | ○ |
| 3.5 | ソフトウェア・アーキテクチャ・デザイン・チャート | △ | ○ | ○ |
| 3.6 | デザイン仕様書 | × | ○ | ○ |
| 3.7 | トレサビリティ分析 | × | ○ | ○ |
| 3.8, 4.1 | 開発ドキュメント（ソフトウェア・ライフサイクルに応じた開発計画、コンフィギュレーション・マネージメント及びメンテナンス計画） | × | △ | ○ |
| 3.9 | 検証と妥当性確認テスト（VV&T） | △ | ○ | ○ |
| 3.10 | リビジョン・レベル | × | ○ | ○ |
| 3.11 | 未解決のバグ | × | ○ | ○ |
| 3.12 | バージョン管理番号 | ○ | ○ | ○ |

○　-必要、△-一部必要、×-不要

③現行制度の問題点

2001 年、FDA の保証制度の信頼性が疑われるような事故がパナマで報告されている。Multidata Systems International（本社：ミズーリ州セントルイス）がパナマにある病院に納めた放射線治療装置の放射線放射時間をコントロールするソフトウェアに不具合があり死者 5 名を出す事件が起きた。この事件によって FDA の現行保証制度がドキュメント中心主義の審査で、その審査手法もプログラム審査ツールなどは使わず、すべて人海戦術で行っている実態に問題がないのかという指摘がなされている。

(3)　e-Voting(電子投票システム)

①制度の概要

米国政府の電子投票システムに対する取り組みは長い歴史を持っている。1975 年に National Bureau of Standards（現在 NIST）と Office of Federal Elections（現 Office of Election Administration の前身）が『Effective Use of Computing Technology in Vote Tallying』を発表したことに端を発する。その後、議会は 1984 年に連邦選挙管理委員会（FEC）に対して、電子投票システムに関するスタンダ

ードを作るための予算を配分し、本格的な作業が開始され、1990 年１月に初のスタンダードである『Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems』が発表された。

最新の電子投票システムに関するスタンダードの Federal Voting Systems Standards（FVSS）は 2002 年４月 30 日に FEC によって承認された。FVSS にはシステムのパフォーマンス・スタンダードと検証に関する基準が示されている。ただし、同バージョンの FVSS ではインターネット投票システムや民生用（COTS）ソフトウェアに関する技術については含まれておらず、次期バージョンにむけて継続的に検討されていくことが必要とされている。

②審査機関

電子投票システムの認可プロセスの責任を負っているのが、National Association of State Election Directors（NASED）である。NASED は 1989 年に設立され、FEC や IEEE の代表者に加え、各州政府の電子投票関連部門代表で結成されている。NASED は FEC が作成するスタンダードに沿って、システムが検証されるプロセスを構築。検査機関を組織内ではなく、ITA（Independent Testing Authority）と呼ばれる民間組織に委託するシステムを採用した。現在 ITA として認定されているのは３団体となっている。

NASDA が認定している ITA

| 検証対象 | 企業名 | URL |
|---|---|---|
| ハードウェア | Wyle Laboratories （アラバマ州） | http://www.wylelabs.com/ |
| ソフトウェア | CIBER, Inc （アラバマ州） | http://www.ciber.com/ |
| | SysTest Labs, LLC （コロラド州） | http://www.systest.com/ |

③現行制度の問題点

認定済 e-Voting システムが実際に利用される機会が増えるにつれ、システムの信頼性に対する問題が次々と明るみに出てきている。

- カリフルニア州サンディエゴでは、タッチスクリーンが正常に起動せず、投票開始時間が 2 時間遅れ、一部の有権者は他の投票所で投票を行わなければならない事態になった。
- ジョージア州では、有権者が Diebold 社製の e-Voting システムのタッチスクリーンで候補を選択すると、選択しなかった方の候補に投票したように記録された。
- フロリダ州の一部地域では、ES＆S 社製システムに問題があり、投票した数百人の有権者が投票していないことになっていた。
- アラバマ州では、コンピュータのバグによって、7 千票にミスが生じ知事選の結果が不透明なものとなってしまった。

こうした現状に対し、現行の検査システムでは信頼性のある投票システムを提供するには不十分であるという専門家の意見が高まっている。州政府の中には、認定済みのシステムに関して証明を取り消したり、システム提供ベンダに対して強制捜査を行ったりという動きに出ているところもある。例えば、カリフォルニア州政府は今年４月に Diebold 社の TSx タッチスクリーン・システムの利用を禁止すると同時に、Diebold 社に対する強制調査を行うと発表している。

ITA の検証制度に依存する仕組みに異を唱える関係者も多い。その理由として、ITA が IT 業界との関係が強すぎるため、政府や利用者にとってフェアな検査を行わないのではないかという疑念があるためである。ジョンズ・ホプキンス大学の Avi Rubin 教授はこの問題の権威として、問題提起を行っている。

電子投票を巡る最近の話題しては、１１月に大統領選を控えた今年 9 月には、米連邦控訴裁判所がフロリダ州において投票記録の残らない電子投票システムの採用の是非を問う訴訟を復活させたことが関係者の関心を集めている。これは Robert Wexler 民主党下院議員をはじめとするフロリダ州選出の議員が今年 3 月に提起した訴訟に関するもので、投票記録の残らないタッチスクリーン式の投票システムでは手作業による再集計が不可能なため、フロリダ州の 15 郡がこのようなシステムを導入するのは違憲であると主張しているものである（フロリダ州フォートローダーデール地裁は手続き上の理由で棄却していた）。

また、今年 9 月下旬には米国コンピュータ機械学会（ACM=Association for Computing Machinery）は、電子投票システムの危険性を警告し、投票記録の残らないシステムを選挙で使用しないように警告を出している。

## ４．ソフトウェア品質を向上させるための研究開発

政府による取り組みに加え、ソフトウェア品質改善に向けた様々な研究開発が、産学官連携コンソーシアムや、大学、企業などで行われている。

### (1)　産学官共同プロジェクトによる取り組み

#### ① Sustainable Computing Consortium(SCC)

SCC は 2003 年 10 月にカーネギーメロン大学に設立された Cylab という研究所が中心となって設立されたコンソーシアムである。米国のソフトウェアの品質向上を目指すために、IT 企業、ユーザ企業、米政府など 30 のステークホルダー機関が結集した。ファイザー、アルコア、レイシオンなど問題意識の高い多業種からなる有力ユーザ群のみならず、セキュリティの側面からソフトウェア問題に取

り組む NSA や NASA などの政府機関も参画している。IT 企業からは、シスコに加え、バグ問題では知名度の高いオラクルとマイクロソフトも参加している。

現在以下の２つのワーキング・グループが展開されている。

＜Artifact Measurement and Software Measurement Testbed＞
現在普及しているプロセス重視のソフトウェア・テスト（CMM、ISO-9000、Rational Unified Process、Extreme Programming など）はソフトウェアのバグを完全に取り除くには不十分であると考え、ソフトウェアの完成品を検査し、そのパフォーマンスを評価する検査システムを作り出すことを目指している。最終的ゴールは、現在の試験・プロセス制度を補完できるグローバル･スタンダードとなりえるソフトウェアの検査手法を編み出すこととしている。

＜Risk Management and Risk Management Intellectual Framework＞
リスク・マネージメントに関する同ワーキング・グループでは、ソフトウェアの品質問題によって生じるビジネス上のリスクや経済インパクトについて、各種調査研究を行うことを目的としている。

② Software Engineering Research Center (SERC)

SERC は米科学財団（NSF）の産学協同リサーチ・センター（Industry/University Cooperative Research Center）の 1 つのプロジェクトとして 1986 年に発足した。NSF は同センターによって、科学技術の研究開発における産学の長期的パートナーシップの構築を目指している。産業界は同センターの研究開発に対して、資金的協力を行うだけでなく、企業研究者の大学研究へのフィードバックや、大学の研究開発に役立つ実地データの提供を行うことになっている。一方、大学側は学内の最先端研究設備を利用し、あまりに先端的過ぎるために企業研究室では実施できないような研究開発を行い、その成果を産業界に提供することを使命としている。SERC はこの協同リサーチ・センターの中で唯一ソフトウェアエンジニア部門に関わるプロジェクトである。

SERC の研究対象は多岐にわたり、ソフトウェア品質に関わる研究の例としては、パデュー大学を中心にデューク大学、ジョージ・ワシントン大学、ブラジルにあるサンパウロ大学などが協同で「Architecture Based Estimation of Software Reliability and Testing Distributed Systems」という研究が行われている。ここでは、ソフトウェア信頼性の評価をシステムの完成品を対象として行うのではなく、コンポーネント・ベースで、ソフトウェア・ライフサイクルの早い段階から評価を行うべきという CBRE（Component-Based Reliability Estimation）の研究を行っている。

③ Software Engineering Laboratory (SEL)

SEL はメリーランド大学、NASA/Goddard 及び Computer Science Corporation (CSC)という産官学のジョイント・ベンチャーとして設立された。現在の中心的な研究テーマとしては、軍事や宇宙開発への民生用（COTS）ソフトウェアを利用する場合の信頼性研究とソフトウェアのバグを発見技術に関する研究の二本柱がある。COTS に関する研究では、NASA のシステム開発に利用可能と考えられる COTS ソフトウェアの評価方法や、COTS ソフトウェアを導入する際のベスト・プラクティスの検討を行っている。ソフトウェアのバグ発見技術に関しては、ソフトウェアの不具合を開発の早期に発見することで、ソフトウェアの品質向上と同時に開発コストの削減を目的として、それを効率的に実現するためのメソッドの研究を行っている。

(2)　大学における取り組み

①カーネギーメロン大学　ソフトウェア工学研究所(SEI)

SEI はソフトウェア・プロセスの成熟度モデルである CMM（Capability Maturity Model）の開発で有名である。SEI はこれまで、質の高いソフトウェアを、納期・予算内で効率的に開発するための技術の追求を目標に掲げて、開発プロセス重視の CMM をはじめ各種の研究を行ってきた。米国におけるソフトウェア品質向上の研究を行う機関としては、最も先端的な研究所のひとつとして名高い。SEI は DOD と連携したプロジェクトを遂行していることでも知られている。

CMM関連の最新の研究としては、2004 年 2 月にTom Bernard（米国空軍 航空システムセンター）、 Brian Gallagher (SEI)、 Roger Bate (SEI)、Hal Wilson（Northrop Grumman社）が発表した『CMMI Acquisition Module （CMMI-AM） Version 1.0』というレポートがある。同レポートでは、政府機関がCMMIを効率的かつ効果的な導入を成功させるためのベスト・プラクティスが示されている。同時に、政府機関だけではなく、民間企業においても応用可能なプラクティスとして紹介されている。また、昨年 10 月にDennis R. Goldenson とDian L. Gibsonによって発表された『Demonstrating the Impact and Benefits of CMMI: An Update and Preliminary Results』では、CMMIを導入を成功させた米国、欧州、オーストラリアの 12 のケースについて、５つの指標（コスト、スケジュール管理、品質、顧客満足度、投資対効果）を用いた分析が行われている。

SEI の CMM 以外のソフトウェア品質向上関連プロジェクトとしては以下のようなものがある。

SEI のソフトウェア品質向上関連プログラムの例

| タイトル | 概要 |
|---|---|
| **Performance-Critical Systems (PCS) Initiative** http://www.sei.cmu.edu/pcs/pcs.html | PCS (Performance-Critical Systems) Initiative で はソフトウェアのパフォーマンスや信頼性を予測可能にする研究に焦点をあてている。<br><br>主なプロジェクト：<br>♦ Model-based Real-time System Design and Analysis<br>♦ Dependable Software-based Systems |
| **Predictable Assembly from Certifiable Components (PACC)** http://www.sei.cmu.edu/pacc/ | PACC では、現在広く用いられているコンポーネント・ベースのソフトウェア・エンジニアリング・プロセスやツールを超える次世代ソフトウェア開発技術の研究開発を行っている。 |

## ②メリーランド大学　Fraunhofer Center for Experimental Software Engineering

Fraunhofer Center for Experimental Software Engineering はソフトウェア・エンジニアリング、ソフトウェア開発プラクティス、ソフトウェア・プロセスなどの研究拠点として、独 Fraunhofer が独以外にもつ世界５７ヶ所の拠点の一つとして、1998 年にメリーランド大学内に設立された。

ここでは、単に理論だけを追うのではなく、学生・研究者が実際のアプリケーション開発を経験することを通じて、ソフトウェア開発現場での技術向上を模索している。

ソフトウェア品質向上に向けた研究の例としては以下のようなプロジェクトがある。

Fraunhofer Center for Experimental Software Engineering における研究例

| プロジェクト・タイトル | 概要 |
|---|---|
| **High Dependability Computing Project (HDCP)** (http://fc-md.umd.edu/fcmd/Apps/ProjectsRecord.asp?ID=9) | HDCP は、高い信頼性のあるソフトウェア開発を NASA との協力体制の下で行っている。HDCP で開発された新たなソフトウェア・デザインや開発手法は、単に机上論でおわることなく、NASA の施設において実証試験が行われ、より実用性の高い技術として完成されることを目的としている。<br><br>パートナー：NASA, Carnegie Mellon, University of Maryland, Fraunhofer Center Maryland, University of Southern California, Massachusetts Institute of Technology, University of Washington and University of Wisconsin. |
| **Reading/Inspection Technologies** (http://fc-md.umd.edu/fcmd/Apps/ProjectsRecord.asp?ID=1) | 同プロジェクトでは、ソフトウェア・ライフサイクルに応じたソフトウェア・プログラミングのコード解読技術の開発・改良によってソフトウェア・バグを軽減する取り組みを行っている。<br><br>パートナー：University of Maryland, Maryland, USA<br>Federal University of Rio de Janeiro, Rio de Janeiro, Brazil |
| **Dynamic Modeling and Simulation of the System Testing Process** （http://fc-md.umd.edu/fcmd/Apps/ProjectsRecord.asp?ID=10） | ソフトウェア開発ライフサイクルの最終段階であるシステム検証を効率的に行うことで、品質の高いソフトを開発しつつ、コスト削減・時間短縮を図る取り組みを Motorola と協力して行っている。<br><br>パートナー：Motorola, Inc., Illinois, USA |

③ジョージア工科大学　Aristle Research Group

ジョージア工科大学の Aristle Research Group では、ソフトウェア・エンジニアリングの中でも、ソフトウェア開発・試験・維持管理といったソフトウェア・ライフサイクルのあらゆる局面を自動化させるツールの研究・開発に焦点をあてている。

その中にソフトウェア品質を向上させるためのプロジェクト GAMMA: Continuous Evolution of Software after Development が展開されている。GAMMA では、ソフトウェアが出荷された後に、恒常的にソフトウェアのパフォーマンスをモニタリング・分析し、問題の迅速な対処を行うことによって品質向上を目指しており、そのための自動化ツールの研究を行っている。

(3)　企業における取り組み

企業のソフトウェア改善に向けた取り組みも活発になってきている。先にあげたコンソーシアムなどの参加のほか、社内での研究活動を推進することによって改善を図る従来からの研究開発パターン（Microsoft）に加え、オープンソースの思想を生かして、なるべく多くの開発者を取り込むことによって、開発ツール及びソフトウェアの改善を図ろうとする取り組み（Sun Microsystems や IBM）も始められている。

①　Microsoft

プログラムのバグに関する問題で槍玉に挙げられるマイクロソフトであるが、トップ・ソフトウェア企業として、ソフトウェア品質の向上については早くから真剣に取り組んできた歴史がある。その中心的役割を担っているのが、Program Productivity Research Center (PPRC)である。PPRC では特にソフトウェア品質向上を目指す 2 つのグループが活躍している。

＜Program Analysis Research Group＞

Program Analysis Research Group では、Microsoft のプログラム開発チームの品質改善を支援するための研究を行うのと同時に、プログラム分析の分野の先端技術の研究も行っている。

Program Analysis Research Group が研究開発対象とするツール例

| 研究対象ツール | 概要 |
|---|---|
| Detailed Symbolic Simulation (PREfix) | バグ発見ツールの PREFix は当初 Intrinsa によって開発された。1999 年に、Microsoft は Windows2000 のバグ問題解決に向けて、Intrinsa を合併。合併費用は 60 億ドル以上に達したと見られている。PREFix はこれまで、Windows 関連商品に潜む数千個のバグを発見してきた。 |

| | |
|---|---|
| Path-Sensitive Dataflow Analysis (ESP) | 統計データに基づくデータ・フロー分析を基礎としたソフトウェア検証ツール。 |
| Annotation-Based Software Validation (espX) | コンパイル時のバッファ・オーバーランを検地するためのツール。espX の利用によって、プログラマーの労力軽減、注釈自動生成などが可能である。 |
| Efficient Local Analysis (PREsharp) | C/C++言語で書かれたプログラムのバグを発見するツール。 |
| Post-mortem Analysis (PSE). | ソフトウェア・プログラムについて発生した問題を事後的に解析するツール。 |

＜Reliability Group＞

同グループでは、Microsoft のプログラム開発の初期段階において、不具合を発見し、開発・検証サイクルの効率化を目指している。プログラム内の注釈記述方法改善、統計データに基づいたバグ修正機能、及び開発・検証技術のベストプラクティス収集などを中心に研究を行っている。

Reliability Group が行っている研究プロジェクトの例

| プロジェクト | 概要 |
|---|---|
| Software Productivity Tools (SPT) | ソフトウェア・デザイン、開発、デバッグ、検証といったソフトウェア・ライフサイクルをより効率化するための次世代ツールの開発に焦点を絞ったプロジェクト。 |
| Error Detection Via Scalable Program Analysis (ESP) | C/C++プログラムにあるプロトコール・エラーを統計データをもとに発見するメソッド（ESP）の研究開発を行っている。 |
| PREfast Intra-procedural Source Code Analysis | PREfast はプログラム開発者が特定のバグをソフトウェア中に書き込まないように防止するツールで、Microsoft 製品開発の現場で今日使われている。同プロジェクトでは同ツールの研究開発を行っている。 |
| PREfix Scalable, Path Sensitive Source Code Analysis | C/C++言語プログラムのバグ発見ツール PREfix に関するプロジェクト。 |
| Scout - Test Prioritization System | ソフトウェア・テストにおいて、新規・修正箇所を優先的に行う技術の研究を行っている。 |
| RCA - Defect Root Cause Analysis | ソフトウェア・バグ発生の根本的原因を追究するための分析スキーマ及びメソッドの研究開発を行っているプロジェクト。 |

② Sun Microsystems

Sun Microsystems の研究所 Sun Microsystems Laboratories では Jackpot と名づけられたプロジェクトで、ソフトウェア特に Java によるソフトウェア品質向上をねらった研究が進められている。当プロジェクトは、Sun が独自に開発したプログラム開発ツールの徹底的見直し・改善を行うことで、より使いやすく、より効率的にプログラム・コードの複雑さを減らす開発ツールを作り上げることを目指し、2000 年に始まった。さらに、オープンソースの NetBean プラットフォーム

を活用して、同研究所の中だけではなく、ソフトウェア開発者のコミュニティと情報を共有することによって、開発ツールの改善を促進しようと試みている。

③　　IBM

IBM は Eclipse Foundation という非営利団体を 2001 年に設立して、ソフトウェア品質改善に取り組んでいる。Eclipse は Sun 同様に開発ツール・プロバイダーの誰もがアクセスできるオープンソース・プラットフォームを採用、Microsoft の社内囲い込み戦略と一線を画している。設立には、Borland、MERANT、QNXSoftware Systems、Red Hat などが関わった。現在メンバー企業は HP、Intel、Ericsson などの大手を含め 50 社以上にのぼる。Eclipse 理事の Skip McGaughey は Eclipse の目的について「当プロジェクトのエッセンスは民主主義的なオープンソース・デザイン・プロセスにある。オープンソース環境で大人数が参加したソフトウェア・デザイン・プロセスを採用すると、ソフトウェア品質がよりよいものになる可能性が高くなる」と述べている。

(参考資料)

http://sse.se.rit.edu/Portals/0/cusumano-practice.pdf
http://nist.gov/director/prog-ofc/report02-3.pdf
http://www.informationweek.com/story/IWK20020517S0010
http://www.eweek.com/article2/0,1759,1543652,00.asp?kc=EWNWS030804DTX1K0000005%2099
http://www.hpcc.gov/pubs/hcs-Mar98/HCS_agenda.pdf
http://www7.nationalacademies.org/cstb/project_dependable.html
http://www.sei.cmu.edu/products/events/acquisition/2004-presentations/jarzombek/jarzombek.pdf
http://www.rtca.org
http://www.faa.gov/certification/aircraft/
http://www.fda.gov/cdrh/ode/57.html
http://www.fec.gov/pages/vssfinal/vss.html
http://www.nased.org/
http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2004/03/03/state0339EST0046.DTL
http://www.washingtonpost.com/ac2/wp-dyn/A39241-2003Mar27?language=printer
http://www.washingtonpost.com/ac2/wp-dyn/A42085-2003Aug10?language=printer
http://www.ss.ca.gov/executive/press_releases/2004/04_030.pdf
http://avirubin.com/vote/ita.challenge.pdf
http://www.acm.org/usacm/weblog/index.php?p=73
http://www.cylab.cmu.edu/default.aspx?id=8
http://www.cylab.cmu.edu/default.aspx?id=177
http://www.serc.net/web/index.asp
http://www.purdue.edu
http://www.serc.net/web/research/past__projects/projects/mathur/sld001.htm
http://sel.gsfc.nasa.gov/
http://www.csc.com/
http://www.sei.cmu.edu/
http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr001.pdf
http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr009-revised.pdf
http://fc-md.umd.edu/fcmd/index.html
http://www.cc.gatech.edu/aristotle/Research/index.html
http://research.microsoft.com/research/detail.aspx?id=3
http://www.sun.com/2002-1112/feature/
http://www.eclipse.org

http://www.technologyreview.com/purchase/pdf_dl.asp?79juh=910351&hy6f0=6799
このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。