鉄道用高安全ソフトウェアに関する調査研究

日本大学 理工学部 応用情報工学科 准教授　高橋 聖

１．はじめに

鉄道システムには様々なところでコンピュータが使われている。中でも列車制御システムは，列車の衝突や脱線を防ぎ，列車の安全な運行を確保するために重要である。したがって，列車制御システムに用いられるコンピュータシステムは，高い安全性が求められる。コンピュータはハードウェアとソフトウェアで構成される。ハードウェアの安全性は，これまでの研究成果や開発実績により，冗長構成を主とした高安全なハードウェア技術が確立されている。一方ソフトウェアの安全性は，潜在的なバグなどにより，その故障状態を予測することは困難である。鉄道システムのソフトウェアの安全性に関する検討はこれまでもなされているが，より高安全で効率の良いソフトウェア開発をするためには，さらなる技術開発・適用を進める必要がある。本調査研究では，日本における鉄道用高安全ソフトウェアの研究動向を文献により明らかにし，今後の課題について考察することを目的とする。

２．調査方法

日本の論文検索ポータルサイトである CiNii により，鉄道用高安全ソフトウェアに関する文献を検索した。CiNii（サイニィ）は，NII（国立情報学研究所）論文情報ナビゲータのことで，論文や図書・雑誌などの学術情報で検索できるデータベース・サービスである [(1)]。本調査研究では，CiNii のサービスの一つである「CiNii Articles」により，鉄道用高安全ソフトウェアに関する文献を検索した。CiNii Articles は，日本の論文を探すためのデータベース・サービスで，学協会刊行物・大学研究紀要・国立国会図書館の雑誌記事索引データベースなどの学術論文情報が約 1,500 万件（2011 年 10 月 1 日時点）収録されている。

検索条件として，「鉄道，ソフトウェア，安全」の３つのキーワードで AND 検索を行った。検索においては，タイトルや出版年などの詳細検索の限定条件は付加していない。安全にかかわるシステムの「高信頼化」は，しばしば「高安全化」につながるので，検索条件として，「鉄道，ソフトウェア，信頼」の３つのキーワードでの AND 検索も行ってみた。その結果，これらのキーワードで検索された文献のうち，鉄道用高安全ソフトウェアに関する文献として抽出したものは，すべて「鉄道，ソフトウェア，安全」の３つのキーワードで検索・抽出された文献の中に含まれていた。

「鉄道，ソフトウェア，安全」の３つのキーワードで検索された文献の内容を調査し，これらの中から鉄道用高安全ソフトウェアに関して論じているものを調査対象文献として抽出した。検索時に詳細検索の限定条件を付加していないので，３つのキーワードで検索された文献の中には，本調査研究での調査対象以外の文献も含まれてしまうからである。

抽出した鉄道用高安全ソフトウェアに関する文献を，その内容から「手法提案」，「適用事例」，「動向調査」の３つに分類した。手法提案に分類したものは，高安全なソフトウェアの構成法や，安全性の検証手法の提案など，新たな手法を提案することが主目的の文献が含まれる。適用事例に分類したものは，

新たな手法の提案はなされていないが，既存の手法を具体的な鉄道システムに適用することで，安全性の向上に寄与することを示した文献が含まれる。動向調査に分類したものは，高安全なソフトウェアの構成技術の解説や動向紹介，国際規格の動向調査を主目的とした文献が含まれる。

3．調査結果

3．1　全体の傾向

CiNii Article により，「鉄道，ソフトウェア，安全」の 3 つのキーワードで検索された文献の総数は 55 件であった（2014 年 3 月時点）。これらの中から鉄道用高安全ソフトウェアに関して論じているものとして抽出したのは，1995 年から 2013 年までの 36 件であった [(2) ~ (37)]。図 1 に，内容分類別・鉄道用高安全ソフトウェアに関する文献数の年次推移を示す。2006 年から 2008 年の 3 年間を除き，毎年数件ごとの文献が発表されている。

「手法提案」,「適用事例」,「動向調査」の各分類の件数はほぼ同じ割合で, それぞれ 13 件 [(2) ~ (14)], 10 件 [(15) ~ (24)]，13 件 [(25) ~ (37)] であった。「手法提案」および「動向調査」に関する文献のほとんどは，2005 年以前に発表されている（それぞれ 13 件中 11 件）。特に「動向調査」は，2001 年から 2005 年の 5 年間に集中している（13 件中 8 件）。これは，鉄道信号の安全性に関する国際規格が，2000 年代の初めに相次いで制定されたことに関連すると考える。これに対し「適用事例」は，2009 年から 2013 年の 5 年間に集中している（10 件中 6 件）。これは最近の傾向として，従来提案された高安全化のための手法を，単に理論としてではなく，実践的な応用に向けて組み入れる努力とみられる。

文献の発行機関は 7 つあり, 図 2 に示すように, それぞれ情報処理学会（1), 鉄道総合技術研究所（2), 電気学会（2)，電子情報通信学会（22)，日本信頼性学会（6)，日本ソフトウェア科学会（1)，日本鉄道電気技術協会（2）であった（括弧内は文献件数を示す)。文献数の約 6 割が電子情報通信学会からの発表が占めている。電子情報通信学会の研究会には，フォールトトレラントシステム研究会，安全性研究会，ディペンダブルコンピューティング研究会など，高安全なソフトウェアに関連する研究会が多く，

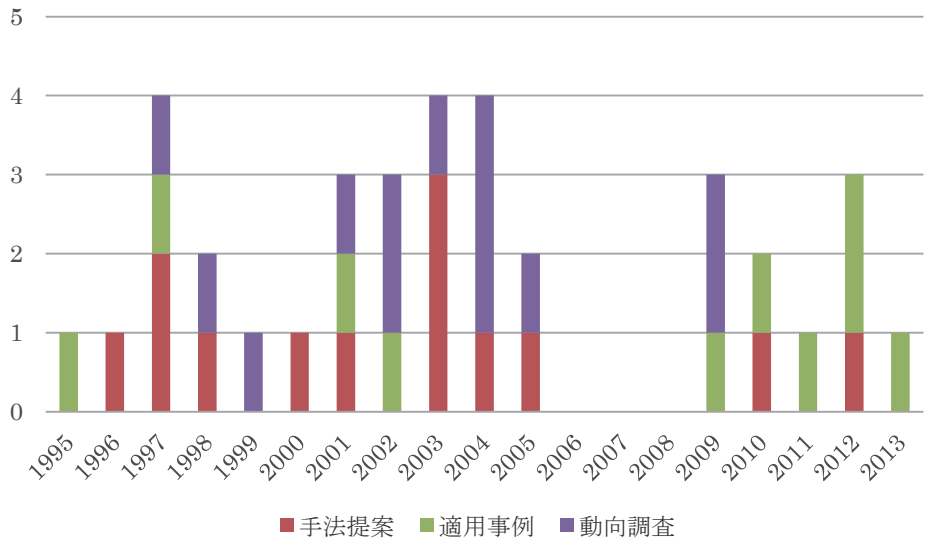

図 1　内容分類別・文献数の年次推移

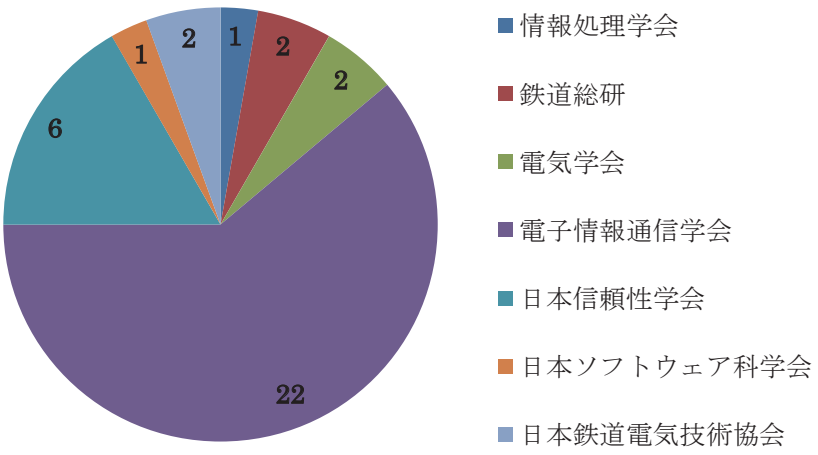

図２　発行機関別文献数

特にディペンダブルコンピューティング研究会では鉄道システムの信頼性・安全性に関する研究発表が精力的に行われている（22 件中 9 件）。次いで日本信頼性学会からの文献が多くなっている。

３．２　内容分類ごとの特徴

「手法提案」,「適用事例」,「動向調査」の 3 つの内容分類ごとに，その特徴を分析した。

「手法提案」の中の高安全なソフトウェアの構成技術として，伊藤ら [8] はイベントチェッカと名づけた安全機構を，オブジェクト指向ソフトウェアのソフトウェアパターンとしてパターン化し，連動装置モデルへの実装例を示した。また森ら [2] は，鉄道信号保安装置向けの次世代 OS として「排他ダブル・スレッド OS」を提案し，従来技術の中核であるシングル・スレッド方式の OS の限界を超えた機能を実現している。安全性評価手法の提案に関しては，岩田ら [6] が，バリス式列車検知型閉そく装置（COMBAT）を対象に，Windows OS の 1 台のパソコン上でシミュレーションによる安全性検証する手法を提案している。

「適用事例」の中では，寺田ら [15],[16],[19],[20] を中心にフォーマルメソッドの鉄道信号分野への適用が多く報告されている。フォーマルメソッドとは，システムの仕様を数学的な背景を持つ仕様記述言語で記述し，コンピュータを利用して，その仕様の妥当性や正当性を検証する手法である。また宗方 [21],[22] は，電子連動装置用ソフトウェアの開発に，国際規格である IEC61508（電気・電子・プログラマブル電子安全関連系の機能安全）を適用した時の効果について報告している。これは，IEC61508 制定の初期における報告で，国際規格に準拠することでソフトウェアの信頼性を客観的に評価できることを示し，その後に国際規格への対応を迫られる産業界に，貴重なデータを提供したことにおいて意義がある。

「動向調査」では，中村ら [33] が，2002 年時点での鉄道におけるディペンダブルソフトウェアの現状について広くサーベイしている。そこでは，鉄道信号用ソフトウェアの開発方針として古くから用いられており，その実績も確認されている代表的な事柄が示されている。例えば，マルチタスクの排除や，アプリケーション処理中の割り込み禁止などがこれにあたる。また, N- バージョンプログラミングなど，ソフトウェアに依拠した安全性確保手法についても解説されている。国際規格に基づいた高安全ソフト

ウェアの開発に関するものとしては，例えば岩田ら[28]が，IEC62279（鉄道信号におけるソフトウェアの安全性規格）に基づく鉄道信号用ソフトウェアの開発について述べており，ソフトウェア開発時の各段階についての概要も説明されている。

４．まとめ

日本における鉄道用高安全ソフトウェアの研究動向を文献により調査した。日本の国内の学術論文データベース・サービスである CiNii Article により検索・抽出した結果，列車制御システムの高安全ソフトウェアに関する文献が 36 件あった。新しい手法提案や，手法の適用事例，国際規格に基づいた開発事例の動向調査等が報告されていた。技術の進化のために新しい手法提案は歓迎すべきであるが，フォーマルメソッドのような，これまでに提案された手法を，実際の開発にいかに適用していくかが，今後重要であると考える。今後の調査研究の課題として，鉄道信号メーカ等の開発実態の把握や，海外の研究動向も調査していきたい。

以上

参考文献

(1) http://ci.nii.ac.jp/
(2) 森 昌也，中村 英夫“鉄道信号保安ソフトウェアの特徴と次世代 OS,”日本信頼性学会誌，34，6，pp.405-410，2012.8
(3) 岩田 浩司，渡辺 郁夫“列車制御システムソフトウェア要求仕様の安全確認項目の設定による誤り低減の検討,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング ，110，333，pp.37-42，2010.12
(4) 寺田 夏樹，高橋 一裕，荻野 隆彦“段階的詳細化によるシステムの高信頼化手法,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング ，105，458，pp.1-6，2005.12
(5) 島添 敏之，畑 好之“鉄道信号システムのコンフィギュレーションにおける XML の活用,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング，104，533，pp.11-18，2004.12
(6) 岩田 浩司，西堀 典幸，平尾 裕司“列車保安制御用ソフトウェアの検証法の検討 : COMBAT を対象とした解析,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング，103，535，pp.15-22，2003.12
(7) 清野 貴博，緒方 和博，二木 厚吉“項書換えを用いた安全性検証の組織化,”コンピュータソフトウェア，20，5，pp.444-457，2003.9
(8) 伊藤 清人, 小林 洋“リアクティブシステムのシナリオチェックにかかわるソフトウェアパターン,”電子情報通信学会論文誌 . A, 基礎・境界，J86-A，7，pp.749-757，2003.7
(9) 伊藤 清人，小林 洋“リアクティブシステムの安全性に関わるソフトウェアパターンの研究,”電子情報通信学会技術研究報告 . SS, ソフトウェアサイエンス，101，359，pp.17-24，2001.10
(10) 奥村 幾正，渡辺 俊勝，伊藤 昇，三平 律雄，SHUMACHER Manfred“安全 PLC を活用した鉄道

信号用連動装置のソフトウェア構成法,”電気学会論文誌 . D, 産業応用部門誌，120，1，pp.88-95，2000.1
(11) 増田 直弘，中村 英夫“システムの安全性評価とソフトウエア高信頼化への応用,”電子情報通信学会技術研究報告 . FTS, フォールトトレラントシステム，98，368，pp.17-24，1998.10
(12) 山田 茂，得能 貢一，笠野 有“ソフトウェア安全性 / 信頼性の定量的評価モデルに関する考察,”電子情報通信学会論文誌 . A, 基礎・境界，J80-A，12，pp.2127-2137，1997.12
(13) 駒嵜 克郎，岸 知二，川口 晃“安全性ソフトウェアのための監視手法の開発,”電子情報通信学会総合大会講演論文集 1997 年 . 情報システム (1)，pp.235，1997.3
(14) 岸 知二，川口 晃，駒嵜 克郎“ソフトウェアアーキテクチャに基づく安全性ソフトウェアの開発,”情報処理学会研究報告 . ソフトウェア工学研究会報告，96，112，pp.49-56，1996.11
(15) 寺田 夏樹，遠山 喬“信号設備の安全性に関する仕様検証手法の適用検討,”鉄道総研報告，27，2，pp.35-40，2013.2
(16) 寺田 夏樹“VDM の紹介と鉄道信号への適用例,”日本信頼性学会誌，34，6，pp.384-389，2012.8
(17) 謝 国，黒田 智也，望月 寛，高橋 聖，中村 英夫“ATP 閉そくシステムの仕様妥当性のモデルベース検証,”電子情報通信学会技術研究報告 . SSS, 安全性，112，52，pp.17-20，2012.5
(18) 井上 淳太，田口 研治，相馬 大輔“5-3 IEC61508 に則ったシステム安全に関する取り組み,”信頼性シンポジウム発表報文集 2011_ 秋季，24，pp.75-78，2011.11
(19) 寺田 夏樹“モデル検査法による単線自動閉そく装置の検証,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング，110，333，pp.31-35，2010.12
(20) 寺田 夏樹“B メソッドによる単線自動閉そく装置の検証,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング，109，334，pp.31-36，2009.12
(21) 宗方 江一郎“鉄道信号分野のソフトウェア開発における安全関連国際規格の有用性検証,”電気学会論文誌 . D, 産業応用部門誌，122，7，pp.693-702，2002.7
(22) 宗方 江一郎“安全関連の国際規格に準拠して開発した電子連動装置ソフトウェアの実践評価,”日本信頼性学会誌，23，7，pp.677-687，2001.11
(23) 福田 光芳，渡辺 郁夫，平尾 裕司“鉄道分野での高信頼性データベースの設計に関する一考察,”電子情報通信学会技術研究報告 . FTS, フォールトトレラントシステム，97，98，pp.41-48，1997.6
(24) 荻野 隆彦，松本 真吾“鉄道における高安全性ソフトウェアへのフォ - マルメソッドの適用,”鉄道総研報告，9，5，pp.37-42，1995.5
(25) 中村 英夫“安全性に配慮した鉄道信号用 OS の変遷と動向,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング，109，334，pp.25-29，2009.12
(26) 中村 英夫“情報システムの信頼性・安全性：モノレール事故が明らかにしたソフトウェアの安全性,”日本信頼性学会誌，31，6，pp.388-393，2009.9
(27) 渡辺 郁夫，平尾 裕司“鉄道信号の安全性,”電子情報通信学会技術研究報告 . SSS, 安全性，105，78，pp.17-20，2005.5
(28) 岩田 浩司，渡辺 郁夫，平尾 裕司“国際規格にもとづくディペンダブルソフトウェアの開発手法

について,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング, 104, 533, pp.19-24, 2004.12

(29) 宗方 江一郎“鉄道信号の安全性・信頼性 (6) : 高信頼性ソフトウェアの開発手法,”鉄道と電気技術, 15, 12, pp.81-84, 2004.11

(30) 渡辺 郁夫“鉄道信号の安全性・信頼性 (5) : ソフトウェアの高信頼化,”鉄道と電気技術, 15, 11, pp.86-89, 2004.10

(31) 渡辺 郁夫, 平尾 裕司“列車制御システムにおける安全性技術の動向,”電子情報通信学会誌, 86, 4, pp.264-269, 2003.4

(32) 平尾 裕司“鉄道信号の安全性規格,”電子情報通信学会技術研究報告 . SSS, 安全性, 102, 395, pp.17-20, 2002.10

(33) 中村 英夫, 高橋 聖“鉄道におけるディペンダブルソフトウェアの現状,”電子情報通信学会技術研究報告 . DC, ディペンダブルコンピューティング, 102, 138, pp.1-5, 2002.6

(34) 平尾 裕司, 渡辺 郁夫“鉄道信号の国際安全性規格に関する考察,”電子情報通信学会技術研究報告 . FTS, フォールトトレラントシステム, 101, 505, pp.25-32, 2001.12

(35) 平尾 裕司, 渡辺 郁夫“鉄道信号における安全性技術の展開,”電子情報通信学会技術研究報告 . FTS, フォールトトレラントシステム, 99, 490, pp.43-50, 1999.12

(36) 渡辺 郁夫, 平尾 裕司“列車制御のフォールトトレランス,”日本信頼性学会誌, 20, 5, pp.318-325, 1998.6

(37) 鍛治 勝三“ソフトウェア・セーフティとその規格化の現状 : ソフトウェア工学的観点から,”電子情報通信学会ソサイエティ大会講演論文集 1997 年 . 情報システム, pp.314-315, 1997.8