

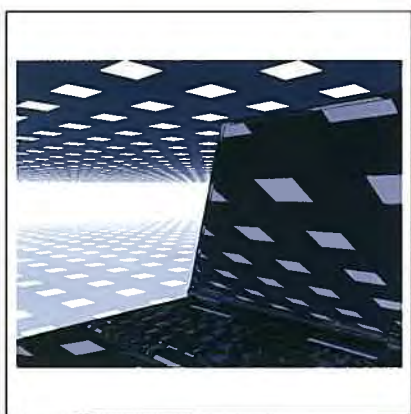
MITSUBISHI

三菱電機技報

Vol.80 No.10

2006 **10**

特集 I 「情報セキュリティシステム/サービス基盤」
特集 II 「設計・開発手法の革新(フロントローディング型開発設計)」



目次

特集I「情報セキュリティシステム／サービス基盤」

三菱電機の暗号研究者たちとの思い出 1
太田和夫

情報セキュリティマネジメント基盤 2
茂木 強・今井直治・速藤 淳

セキュリティ運用を軽快に実現する“MistyGuard”ソリューション 7
青木隆之・田名網淳夫・羽山哲雄

多種多様なログの統合管理を実現する“LogAuditor Enterprise” 11
郡 光則・森田 登・藤村 隆

統合セキュリティ管理サービス 15
太田 潔・田中 朗・藤井誠司・柳原裕之・平井規郎

電子文書の長期原本性保証を実現する“EVERSIGN” 19
宮崎一哉・山中忠和・田中 学

ユーザー情報の多様な変化に対応したアイデンティティライフサイクル管理技術 23
近藤誠一・鶴川達也

ユビキタスセキュリティー監視映像情報セキュリティー 27
山口晃由・山田敬喜・松井 充

特集II「設計・開発手法の革新(フロントローディング型開発設計)」

設計開発プロセスの革新における深層 31
藤田喜久雄

フロントローディング型開発設計への取り組み 32
竹垣盛一・原島忠雄

開発状況の見える化を実現する開発管理システム 35
長江雅史・今村 剛・篠崎順子・川北泰之

社会インフラシステム開発におけるソフトウェア開発プロセス改善 39
安江 悟・風間由美子・川端達明・田中隆行

戦略的再利用に基づくソフトウェア開発 43
小島泰三・辰巳尚吾・原内 聡

カーナビ開発におけるフロントローディング型実装設計 47
小林 孝・船場裕次・片岡秀康・山中康弘・堀越美香

衛星開発における設計／製造品質の向上と効率化 51
川口浩知・佐藤 博・戸塚正弘・石井芳征

車両用モータの熱設計フロントローディング 55
羽下誠司・坂根正道

車載用アナログ混載LSI 59
田中淳也・岩上祐希

大型映像装置におけるGbps高速信号設計技術 63
島崎 陸・高島一樹・諸岡史久

ASIC／FPGAの機能検証技術 67
上野 仁

Information Security System and Service Infrastructure

Recollections on Collaborating with Cryptographers at Mitsubishi Electric
Kazuo Ohta

IT Platform for Information Security Management
Tsuyoshi Motegi, Naoharu Imai, Jun Endo

“MistyGuard” Solution : Information Security Software Easy to Use
Takayuki Aoki, Atsuo Tanaami, Tetsuo Hayama

“LogAuditor Enterprise” : Integrated Management System for Various Log Data
Mitsunori Kori, Noboru Morita, Takashi Fujimura

MIND Integrated Security Management Service
Kiyoshi Ohta, Akira Tanaka, Seiji Fujii, Hiroyuki Sakakibara, Norio Hirai

EVERSIGN : Long-Term Storage System for Signed Documents
Kazuya Miyazaki, Tadakazu Yamanaka, Manabu Tanaka

Identity Lifecycle Management Technology
Seiichi Kondo, Tatsuya Tsurukawa

Ubiquitous Security—Information Security for Surveillance Camera System—
Teruyoshi Yamaguchi, Keiki Yamada, Mitsuru Matsui

Innovation of Design and Development Process (Front-Loading Design and Development)

Depth in Innovation of Design and Development Process
Kikuo Fujita

Activities for Realization of Front-Loading Product Design
Morikazu Takegaki, Tadao Harashima

Development Management System : Visualization for Status of Development
Masashi Nagae, Tsuyoshi Inamura, Junko Shinozaki, Yasuyuki Kawakita

Software Process Improvement in Social Infrastructure Systems Development
Satoru Yasue, Yumiko Kazama, Tatsuaki Kawabata, Takayuki Tanaka

Strategic Software Reuse
Taizo Kojima, Shogo Tatsumi, Satoshi Harauchi

Front Loading Design of Car Navigation System
Takashi Kobayashi, Yuji Funaba, Hideyasu Kataoka, Yasuhiro Yamanaka, Mika Horikoshi

Improvement of Quality and Efficiency in Satellite Development
Hirochika Kawaguchi, Hiroshi Sato, Masahiro Tozuka, Yoshiyuki Ishii

Front-Loading of Thermal Design for Motor of Railroad Car
Seiji Haga, Masamichi Sakane

Digital-Analog Mixed Signal LSI for Automotive Equipment
Junya Tanaka, Yuki Iwagami

Gbps, High Speed Signal Integrity of Large Visual Display Controller
Mutsumi Shimazaki, Kazuki Takabatake, Fumihisa Morooka

A Functional Verification Method for ASIC and FPGA
Hitoshi Ueno

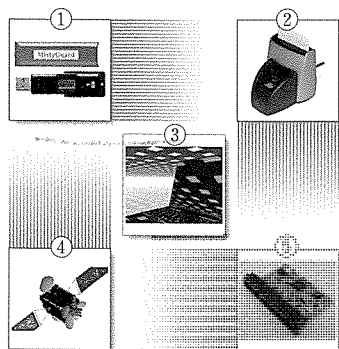
特許と新案

「熱流体CAEシステム」「証明証収集情報生成装置、
証明証検証装置および公開鍵暗号運用システム」 71

「データ変換装置」 72

スポットライト

日本中央競馬会 東京競馬場納め
世界最大のオーロラビジョンLED



*③はイメージ写真。

表紙：情報セキュリティシステム／サービス基盤

MistyGuardソリューションでは、生体認証デバイスとして、指紋照合装置付きのUSBフラッシュメモリ(①)とICカードリーダー(②)をそろえている。ユーザーにおけるセキュリティ意識の高まりによってパスワードは複雑さを要求されているが、指紋照合では、パスワードに頼らない本人認証が可能となることから、その手軽さが受け入れられている。

表紙：設計・開発手法の革新(フロントローディング型開発設計)

メーカーにとって製品設計・開発手法革新によるQCD(Quality, Cost, Delivery)の継続的改善は、製品競争力強化のための最重要課題である。この小特集では、三菱電機におけるフロントローディング型開発設計実現のための取り組みについて述べる。

表紙写真は、三次元CADによる人工衛星構造検証モデル(④)、デジタル・アナログ混載回路シミュレーションを活用して開発したエンジンコントロールユニット(⑤)である。

！ 三菱電機の暗号研究者たちとの思い出

Recollections on Collaborating with Cryptographers at Mitsubishi Electric

太田和夫
Kazuo Ohta

“安心・安全な社会”を目指して情報セキュリティがますます重要になっている。三菱電機を始めとして情報通信機器メーカーや通信事業会社のセキュリティ研究者・技術者は多忙を極め、“嬉(うれ)しい悲鳴”を上げているように見える。この特集号も、このような背景を踏まえて、日ごろの研究開発の成果を世の中にアナウンスするためのものであろう。

電子政府で使用する暗号技術をCRYPTREC (CRYPTography Research and Evaluation Committees) プロジェクトが評価し、「電子政府推奨暗号リスト」を制定した。また、IPA (Information-technology Promotion Agency, Japan) を中心に、「ITセキュリティ評価及び認証制度」や「暗号モジュール試験及び認証制度」が発足し、暗号技術を利用したITセキュリティ製品やシステムの第三者評価の体制も整いつつある。

小生が電電公社時代に暗号研究を開始した25年前を思い出すと、情報セキュリティ分野の盛況には隔世の感がある。当時(1980年代初め)、暗号研究に取り組んでいたのは、国内ではごく少数の組織であった。三菱電機では情報セキュリティグループにおられた井上徹さん(現 広島修道大学教授)と山岸篤弘さんで、私の“暗号研究の同志”であった。創成期の熱気の中、ワークショップで深夜まで議論に熱中したことを懐かしく思い出す。自社の利益はさておき、真実を追究する企業の研究者、行司役として信頼のおける大学の先生方、だれもが自由に意見を交換でき、一種の連帯感が醸し出されていたように思える。今から思えば、“産学連携の理想的な姿”だったと言えよう。

三菱電機の研究所の方々とはこんなことがあった。1990年代初め、NTTは社を挙げてFEAL (Fast data Encipher-

ment Algorithm) というブロック暗号の普及に熱心であった。その安全性評価が私の担当であった。RSA (Rivest, Shamir, Adleman)^(注1)暗号で有名なShamir教授の研究グループがFEALの安全性に問題があることを指摘した(差分解読法)。当然のことながら、NTTの研究所では大騒ぎになった。一方、三菱電機では新進気鋭の松井充さんが、差分解読の追試をこつこつと続けながら、いろいろな観点からFEALの攻撃を試みていた。

日ごろの交流を通じて、松井さんが新しい攻撃(線形解読法)を発見したことを察知した私は、上司に“FEALの安全性評価”のために“三菱電機との共同研究の必要性”を建言した。自社の商品の安全性評価(言い方を代えれば暗号解読)を他社の研究者と行いたいという型破りな提案に対して、GOサインを出した上司は偉かったと思う。それにも増して、三菱電機の部長さんは若輩者の私の話に真剣に耳を傾けて快諾し、励ましてくださった。見識のある方だと、感服した。

さて、小生は5年前に大学に移り、教育者としての人生をスタートした。“社会で通用する研究者、技術者の育成”が目標である。仕事の段取りを自分で整え、自立的かつ自律的に行動できる人材を社会に送り出したいと考えている。“調査・分析”“問題点の発見”“報告書書き”“論文発表”を経験させることにより、“擬似的”成功体験を積み重ねるように努めている。“真”の成功体験は、就職後の企業にお願いすることになる。若者の能力を開花させるべく、人材の一貫教育を実現するための“産学連携”を成功させたいと意気込んでいる。

(注1) RSAは、RSA Security Inc.の登録商標である。

情報セキュリティ マネジメント基盤



茂木 強*



今井直治**



遠藤 淳***

IT Platform for Information Security Management

Tsuyoshi Motegi, Naoharu Imai, Jun Endo

要旨

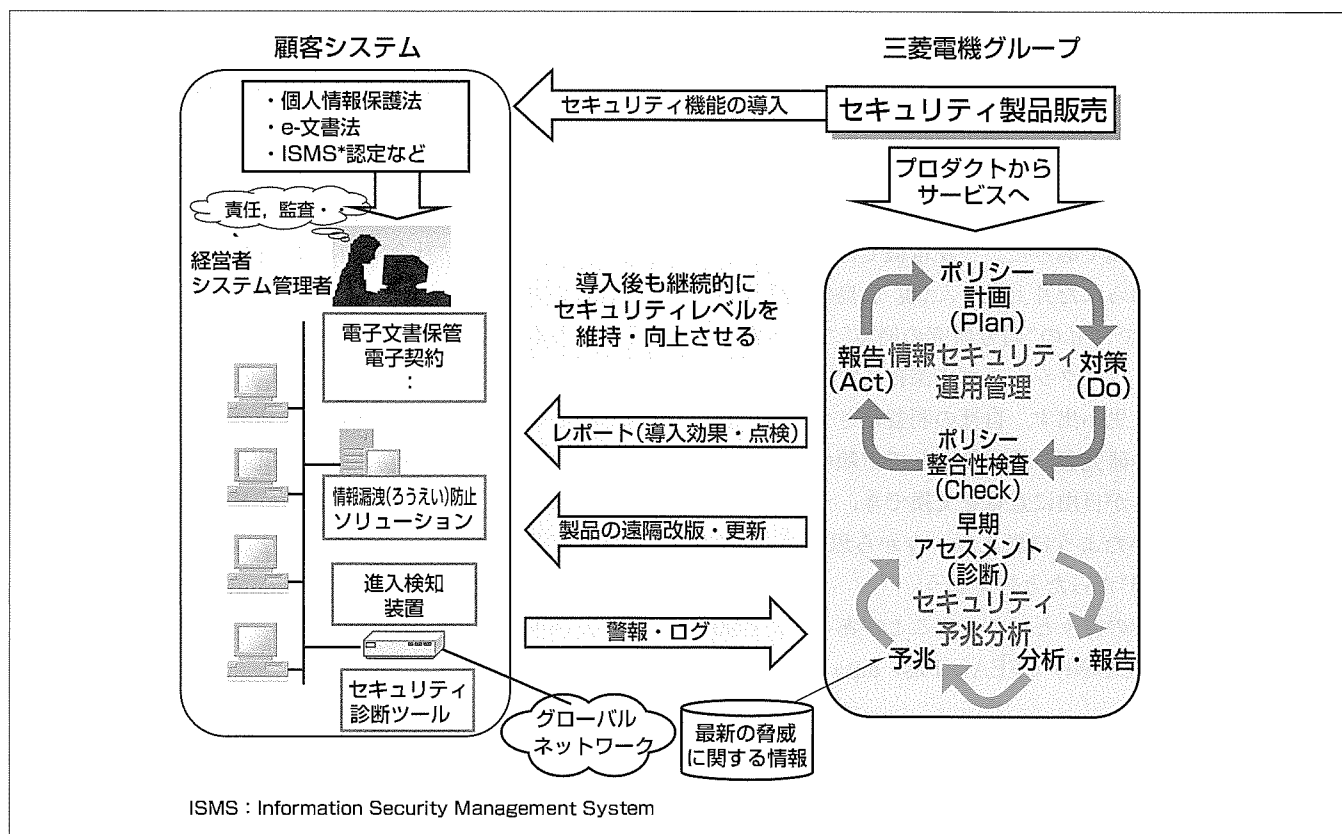
IT利活用の進展に伴い、情報セキュリティ対策の範囲が拡大している。また、新たなセキュリティ脅威は年々増加・多様化の一途をたどっている。このように環境が変化し続ける状況においては、個別のセキュリティ製品を導入しただけでは対策として十分でなく、導入後も継続的にセキュリティレベルを維持する仕組みを構築することが重要な課題となっている。

本稿では、環境の変化を企業・社会の内部と外部とに分けて考えている。内部の変化への対応として、情報システムを構成する“モノ”やソフトウェアの変化を許容するポリシーベースセキュリティ運用管理機能，“ヒト”・組織の変化を許容するロールベースのアイデンティティ管理機能及びそれらの変化を漏れなく記録する大容量ログ機能につい

て述べる。また、外部の変化への対応として、セキュリティリスクの予兆を捕捉してプロアクティブな対応を可能とするセキュリティ予兆分析システムについて述べる。

三菱電機グループでは、情報セキュリティ及び物理セキュリティを体系化し、トータルなセキュリティソリューションを提案してきた。本誌2004年4月号で“情報セキュリティ技術”を、同年8月号で“物理セキュリティ技術”を、2006年4月号で“情報セキュリティマネジメントソリューション”を述べてきたが、今回の特集では、情報セキュリティの継続的な維持向上を顧客へのサービスとして提供するための“情報セキュリティマネジメント基盤”について、全体的な考え方と、個別のソリューション、サービス、コンポーネント技術について述べる。

特集
I



情報セキュリティマネジメント基盤の全体構成

情報セキュリティの脅威は日々進化増大するため、企業や社会の情報システムは、そのセキュリティレベルを常に維持・向上させるための仕組みを必要としている。この特集で述べる情報セキュリティマネジメント基盤は、ポリシーに基づきセキュリティ運用のPDCAを支援するセキュリティ運用管理機能と、攻撃の予兆と対策の提示を行うセキュリティ予兆分析機能とから構成され、顧客システムのセキュリティレベルの継続的な維持・向上に寄与するものである。

1. ま え が き

企業・社会におけるIT利活用の進展に伴い、国家や企業の機密情報から顧客や従業員の個人情報まで様々な情報やデータが電子的に作成され、そのままイントラネットやインターネットを經由して流通し、閲覧・再利用される環境が当たり前となっている。また、個人情報保護法やe文書法の施行など、企業・社会のセキュリティ対策の要請が高まっている。一方、日々進化し続けるウイルスやワームなどの悪意を持ったソフトウェアが様々な経路により企業・社会の情報システムに侵入しようとするなど、情報セキュリティにかかわる脅威は増大の一途である。

このような状況においては、単にセキュリティ製品を導入しただけでは対策として十分ではなく、導入後も継続的にセキュリティレベルを維持する仕組みを構築することが企業・社会にとって重要な課題となっている⁽¹⁾。

本稿では、企業・社会の内外の変化に対応して継続的にセキュリティレベルを維持・向上させる仕組みとしての情報セキュリティマネジメント基盤について述べる。

2. 企業・社会の内部の変化への対応

この章では、企業・社会の内部における変化への対応として、三菱電機グループが提供する“情報セキュリティマネジメントソリューション”の概観と、それを構成するモノやソフトウェアの変化を許容するポリシーベースセキュリティ運用管理機能、ヒト・組織の変化を許容するロールベースのアイデンティティ管理機能、及びそれらの変化を記録・検知する大容量ログ機能について述べる。

2.1 情報セキュリティマネジメントソリューション

三菱電機グループのセキュリティマネジメントソリューションは、ISMS⁽²⁾に従った情報セキュリティ運用管理の枠組みを提供している⁽³⁾。このソリューションは、図1に示すように、ISMSに規定されたPDCA(Plan-Do-Check-Act)の各フェーズで行うべき作業を支援する機能から構成されている。各機能は、資産情報、ID(アイデンティティ)

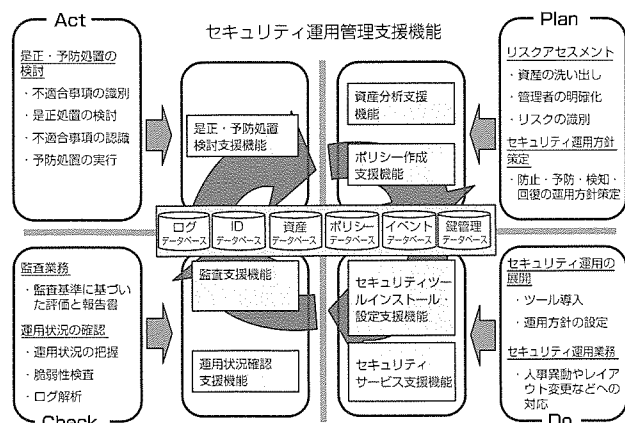


図1. ISMSを支援するセキュリティ運用管理体系

情報、ポリシー情報、イベント情報をPDCAの全フェーズで共有・管理・活用することで、安全かつ効率的なセキュリティシステムの構築と運用を支援する。

具体的なシステムイメージを図2に示す。セキュリティ運用管理は、ISMSのPDCAサイクルにおけるPlan, Do, Checkの作業をIT化することで、セキュリティ運用管理者に対して、確実なセキュリティ運用を可能にする。

2.2 ポリシーベースセキュリティ運用管理

2.2.1 背景と課題

一般にセキュリティ対策として実施されているセキュリティツールやISMSの導入では、運用でのPDCAサイクルによるセキュリティレベルの維持や向上が難しいと言われている。そこで、開発に当たっては、複数社の情報システム関連部門にヒアリングを実施し、以下のような現状のセキュリティ運用の現場における課題を抽出した。

(1) セキュリティ資産管理の作業負荷が高い

セキュリティに関係する資産(ハードウェア、情報)の棚卸(たなおろし)から、廃棄、新規購入、持ち出し状況把握などの管理作業が大変である。

(2) 社内規程や手順に基づいたITシステムに対するセキュリティポリシーの設定が困難

ITを活用したセキュリティ運用手順の策定やセキュリティ対策ツールを活用するためのOS(Operating System)や各種ソフトウェアのセキュリティ設定に対する専門的なスキルがない。

(3) パソコンを中心とした分散環境におけるセキュリティ設定の維持管理が困難

社内に大量に導入されたパソコンに対するセキュリティツールの展開、改版、設定変更の作業が大変である。

さらに、セキュリティ運用ルールの形骸(けいがい)化や、せっかく決めたPDCAサイクルが実現できない場合があるなどの課題も明らかになった。

2.2.2 ポリシーベースセキュリティ運用管理のねらい

以上の課題を解決するために、ポリシーベースセキュリティ運用管理システムを開発した。そのねらいは以下のとおりである。

(1) ポリシーに基づいたセキュリティガバナンスの実現

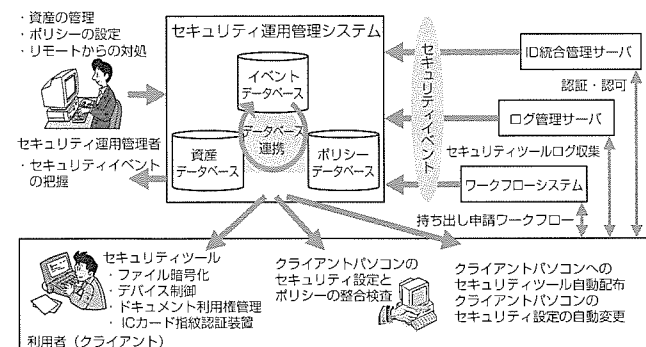


図2. セキュリティ運用管理システムのイメージ

- 配布したセキュリティポリシーを定期的に監査し、IT資産の購入・廃却・持ち出しの際の設定変更や、禁止ソフトウェアのインストールといった不整合を検出し、セキュリティ管理者、利用者、職制管理者に通知する。
- 重大なセキュリティ違反については、違反検出と同時に強制的な再インストールや設定配布までの作業を自動的に行う。

(2) 管理対象システムに対するセキュリティポリシーの維持管理作業の自動化

- パソコンに展開が不可欠なセキュリティツールとそのバージョン、セキュリティに関するOSの設定など、管理対象システムのポリシー実施状況を一括管理する。
- 設定されたセキュリティポリシーに基づいて、ツールのインストールや設定配布を自動的に実施する。

(3) セキュリティ資産管理作業の負荷軽減

- 管理対象システムを構成するハードウェアとソフトウェアに関する資産情報を構成管理データベースで一元管理し、また、データベースを簡便に編集するためのユーザーインターフェースを提供する。

2.2.3 セキュリティポリシー

セキュリティポリシーとは、企業・社会がセキュリティに関して守るべき項目を表現したものである。実際の動作環境(プラットフォーム)に依存しない上位のポリシーと、プラットフォームに依存する動作や設定を規定する下位のポリシーに分けることができる。このシステムで管理するセキュリティポリシーを図3に示す。上位のポリシーに対してプラットフォームに依存した設定配布手段や動作確認手段を関連付けて管理することで、共通のポリシーを規定するだけで、実際には異なるプラットフォーム上のセキュリティ設定の確認や変更を行うことができる。

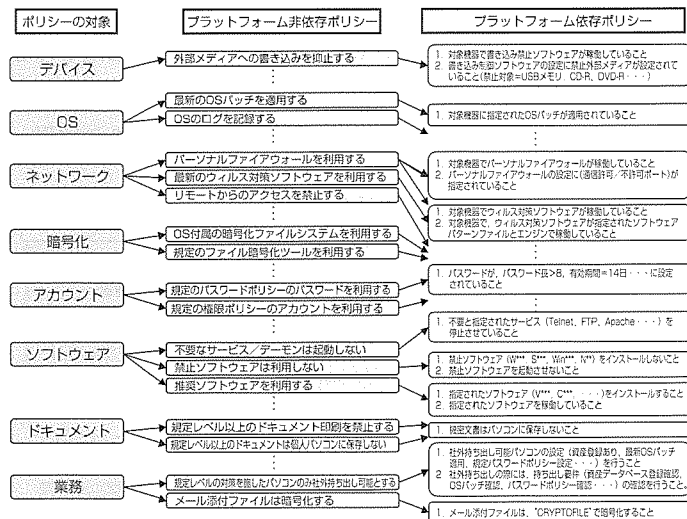


図3. セキュリティポリシーの一覧(抜粋)

2.2.4 ポリシーベースセキュリティ運用管理システム

ポリシーベースでセキュリティを効率的に運用・管理するために、以下の機能を提供する(図4)。

- (1) IT資産管理機能
セキュリティの管理対象となるIT資産の管理機能
- (2) セキュリティポリシー設計機能
セキュリティに関連した社内規程や運用手順に沿ったIT機器のセキュリティ・ポリシー(設定)やポリシー割当ての設計を行う機能
- (3) セキュリティポリシー展開機能
IT機器(パソコン)のセキュリティツールやセキュリティに関連する設定をセキュリティポリシーに基づいて自動的に導入・更新・配布する機能
- (4) セキュリティポリシー監視機能
IT機器のセキュリティポリシー(設定)を定期的に収集・点検する機能
- (5) セキュリティポリシー監査機能
収集したIT機器のセキュリティポリシー(設定)とセキュリティポリシー設計時のポリシー(設定値)を比較し、不整合を検出し報告する機能

2.2.5 セキュリティポリシーの最新化

このシステムを用いたセキュリティポリシーの策定以降も、OSセキュリティパッチの配布、ウイルス情報、新製品のファイル交換ソフトウェアなどが出現する。セキュリティ管理者がこれらの情報を精査し管理対象システムのセキュリティポリシーを最新化する必要があるが、現実には、以下の課題がある。

- 脅威・脆弱(ぜいじゃく)性情報の氾濫(はんらん)
新たな脅威や脆弱性情報は、信頼できる情報や風評デマといったものの類まで実に様々な情報が複数のサイトから発信される。
- 情報セキュリティに対する専門知識やリソースの不足

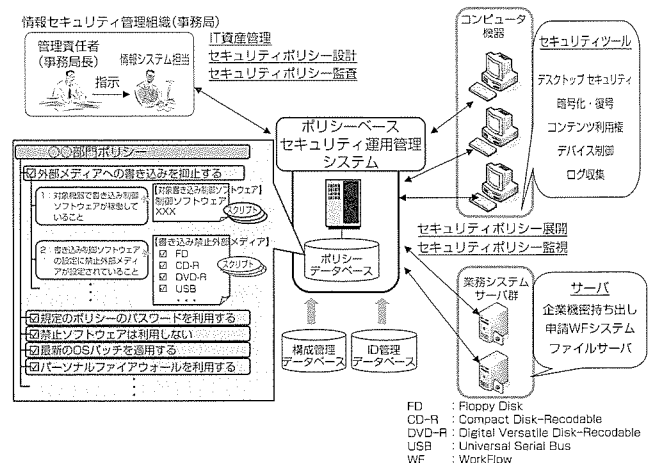


図4. ポリシーベースセキュリティ運用管理システム

収集した脆弱性情報を基に影響度や対策の検討を行うためには、専門的な知識や経験が必要である。セキュリティ管理体制が不十分で専門的な知識を持つ担当者が不在な場合、有効な対策を施すことができない。

このような課題を解決しセキュリティポリシーを最新化していくため、以下の機能を提供し、セキュリティ管理者の意思決定作業を支援する。

(1) 信頼できる外部情報源からの脆弱性情報の収集

公開されている信頼できる最新の脆弱性情報や、これに対するパッチ情報やウイルスパターンファイルなどの情報を収集する。

(2) 影響度の判断と意思決定のための情報提供

上記(1)で収集した脆弱性情報とポリシーベースセキュリティ運用管理システムで設定したセキュリティポリシーを基に、管理対象システムのセキュリティ対策状況を診断し、結果をセキュリティ管理者に報告する。

セキュリティ管理者は、この機能によって提示された診断結果を基に、現在のセキュリティ対策状況の見直しを実施し、ポリシーベースセキュリティ運用管理システムのセキュリティポリシーを再設定することで、セキュリティ運用のPDCAサイクルを実現することができる。

2.3 アイデンティティ管理

アイデンティティ管理システムは、ユーザー情報及びユーザーに割り当てられるアクセス権の管理を行う。ヒト・組織のセキュリティ管理のかなめとなるシステムである。アイデンティティ管理システムの構成を図5に示す。

2.3.1 企業におけるアイデンティティ管理の課題

アイデンティティ管理もまた常に変化にさらされている。企業における変化として以下が挙げられる。

(1) ユーザー情報とアクセスポリシーの変化

入社、退職、異動、昇進、組織変更といったアクセス制御の基になるユーザー情報の属性が変化。また、アクセスの対象機器やコンテンツの追加削除も頻繁に行われている。

(2) ユーザーを識別するための認証デバイスの変化

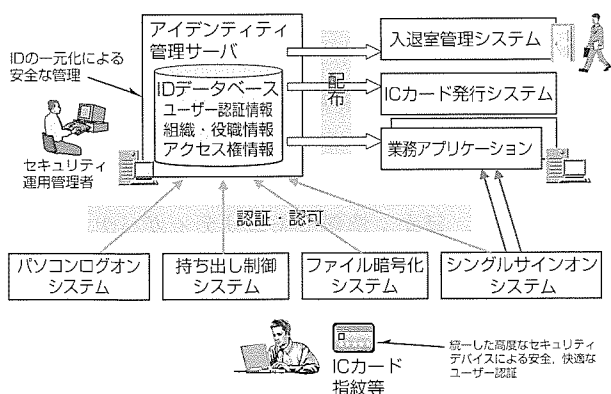


図5. アイデンティティ管理システムの構成

ICカードに代表されるヒトを厳密に識別するためのデバイスには、紛失・汚損・破損・故障・盗難などのリスクにより変化する。

(3) 長期保存された行為ログにおけるユーザーの変化

長期にわたるログの保持期間中にユーザー情報、機器、コンテンツが変化し正しい対応付けができなくなる。

2.3.2 企業向けアイデンティティ管理

以上の課題を解決するために、ロールベースアクセス制御RBAC(Role-Based Access Control)を拡張したモデルを採用したアイデンティティ管理技術を開発した。一般に、階層RBACでは、組織、役職といった人事情報を基にロールを定めることが多いが、人事上の変更がロールとユーザー間の設定に大きな影響を及ぼすという問題があった。これを、人事情報に対応するユーザー、組織をロールから独立させる構造を導入することで解決した。

この結果、人事情報の変更時のロールへの影響度を抑え、企業における人事上の変更を行う担当者とセキュリティポリシーを設定する担当者を分離した運用が可能になった。

2.4 ログの統合管理

2.4.1 セキュリティの観点から見たログの問題

様々な情報システムの生成する大量のログが証拠保全のために蓄積保存されるようになってきた。従来、これらのログは個々の情報システムごとに管理されることが多かったが、ログの種類が増加に伴い、これらのログを統合的に管理し、管理コストの低減や原因分析の効率化を図る必要性が高まっている。

従来のログ管理では汎用のRDBMS(Relational Database Management System)を利用することが多かったが、オンライントランザクションを目的として発達してきたRDBMSは、様々な形式を持ち、長大なデータを含むことの多いログの効率的処理には必ずしも適していない。このため、ログの種類や量の増大に伴い、以下のような問題が見られるようになってきた。

- 異なる形式のログを一元的に取り扱うために事前にデータ形式を統一する必要がある、あらかじめ想定していない形式のログに対応困難
- 蓄積や検索に要する処理時間が長い
- 長期保存に必要なストレージコストが高い

2.4.2 統合ログ管理システム

これらの問題を解決し多様で大量のログの効率的な統合管理を実現した統合ログ管理システムLog Auditor^(注1) Enterpriseを開発した。Log Auditor Enterpriseは、大量に発生する様々な形式のログを収集、蓄積、管理し、統合的なログ分析を実現するための機能を一括提供する。図6に示すように、ログの取り込みを行う定義機能、統合的に

(注1) Log Auditorは、三菱電機インフォメーションテクノロジー(株)の登録商標である。

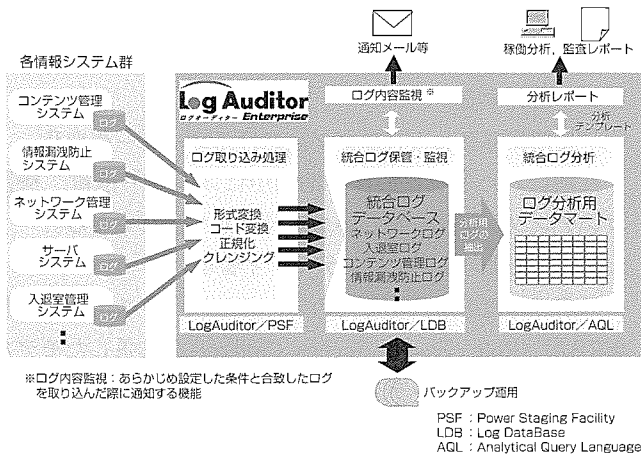


図 6. 大規模統合ログ管理システム

ログを保管・監視するログデータベース，統合的なログの分析エンジンから構成され，さらに，分析フロントとなるMicrosoft^(注2) Excel^(注2) アドインが提供される。

3. 企業・社会の外部の変化への対応

この章では，外部の変化への対応として，セキュリティリスクの予兆を捕捉してプロアクティブな対応を可能とするセキュリティ予兆分析システムについて述べる。

3.1 概要

インターネットを経由した不正アクセスや既知のワーム型ウイルスによる攻撃は，ファイアウォールなどのセキュリティ対策により即座に防御できるが，図7に示すような未知の攻撃は，その被害が顕在化して初めて認知されるため，検知されるまでの期間が長く，有効な対策がとられるまでの間に被害が拡大してしまうのが現状である。未知の攻撃を開始直後に検知できれば，有効な対策をいち早くとることができるため，攻撃による被害の拡大を防止できる。そこで，この課題を解決し未知の攻撃へのプロアクティブな監視サービスを実現するために，未知の攻撃を検出し有効な対策を実施する予兆分析システムの研究開発を進めている。

3.2 セキュリティ予兆分析システム

予兆分析システムは，未知の不正アクセスの予兆を検出する予兆分析アルゴリズムDynamic“SVD(Singular Value Decomposition)”と，その判定結果から早期対策を実現するための機能，及びSIM(Security Information Management)と連携する機能から構成される(図8)。

4. むすび

情報セキュリティの継続的な維持向上を顧客へのサービ

(注2) Microsoft及びExcelは，米国Microsoft Corp.の米国及びその他の国における登録商標又は商標である。

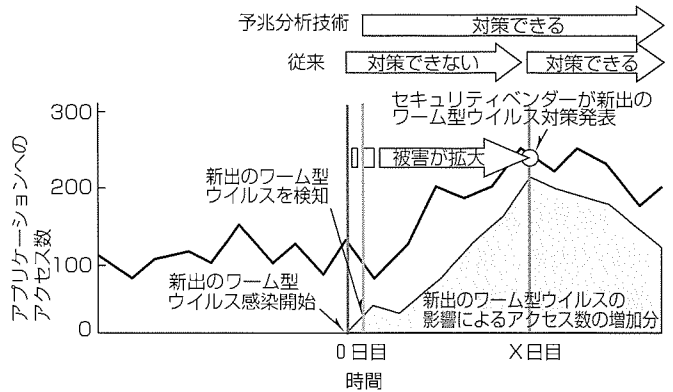


図 7. 未知のワームの検知タイミング

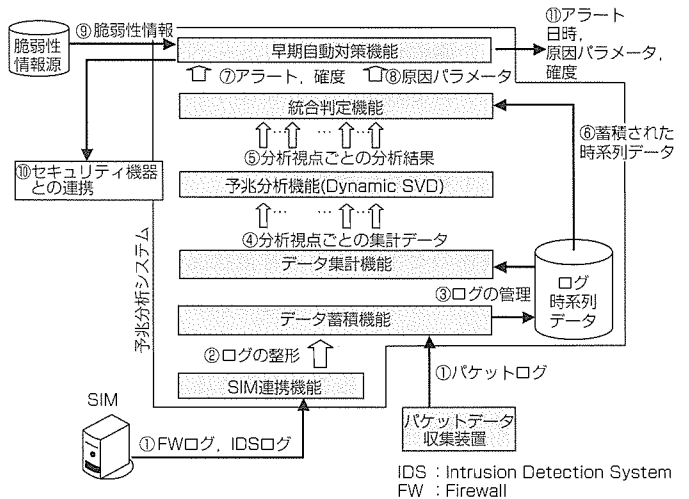


図 8. 予兆分析システム構成

スとして提供するために，企業・社会の内的，外的な変化に対応した統合的な取り組みである“情報セキュリティマネジメント基盤”について述べた。

今後とも，三菱電機グループは，情報セキュリティ，物理セキュリティ，及びそれらを統合したトータルセキュリティのソリューションプロバイダーとして研究開発を継続する。

参考文献

- (1) 青木隆之，ほか：個人情報保護法，e文書法にも対応可能なトータルセキュリティソリューション，三菱電機技報，79，No. 4，279～284 (2005)
- (2) (財)日本規格協会：国際規格ISO/IEC 27001：2005 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，ISO/IEC (2005)
- (3) 遠藤 淳，ほか：情報セキュリティガバナンスを確立する情報セキュリティマネジメントソリューション，三菱電機技報，80，No.4，277～280 (2006)

セキュリティ運用を軽快に実現する “MistyGuard”ソリューション

青木隆之*
田名網淳夫*
羽山哲雄**

“MistyGuard” Solution : Information Security Software Easy to Use

Takayuki Aoki, Atsuo Tanaami, Tetsuo Hayama

要旨

個人情報保護法施行以降、2005年にはP2P(Peer to Peer：不特定多数の個人間でやり取りするインターネットの利用形態)ファイル交換ソフトウェア経由で企業の機密情報が流出する事故が多発して社会問題となったこともあり、ほとんどの企業は何らかの情報セキュリティ対策を導入していると言われている。情報セキュリティツールの利用・運用では利用者及び管理者に負担をかけないことが求められている。

このような背景から、三菱電機インフォメーションシステムズ(株)(MDIS)は、トータルな情報セキュリティ“MistyGuard^(注1)”ソリューションに対して、組織及び個人としての更なる使いやすさ向上を目指し、以下に示すようなバージョンアップを実施した。

(1) ファイル暗号化ソフトウェア“CRYPTOFILE^(注1) PLUS”

これまでは導入時のセキュリティ設定を変更する場合はインストールし直す必要があったが、更新プログラム(アップデート)を実行するだけでセキュリティ設定を変更できるようにした。

(2) パソコンログオンソフトウェア“MISTYLOGON^(注1)

Lite”

これまでは管理用サーバの導入が不可欠であったが、管理サーバがなくても導入可能とした。さらに、指紋照合装置付USB(Universal Serial Bus)フラッシュメモリを使用し、メモリへのアクセスを指紋照合で制御することによって、記録されたデータの安全な持ち運びを可能とした。

(3) 企業機密情報管理“DROSY^(注2) Enterprise Edition”

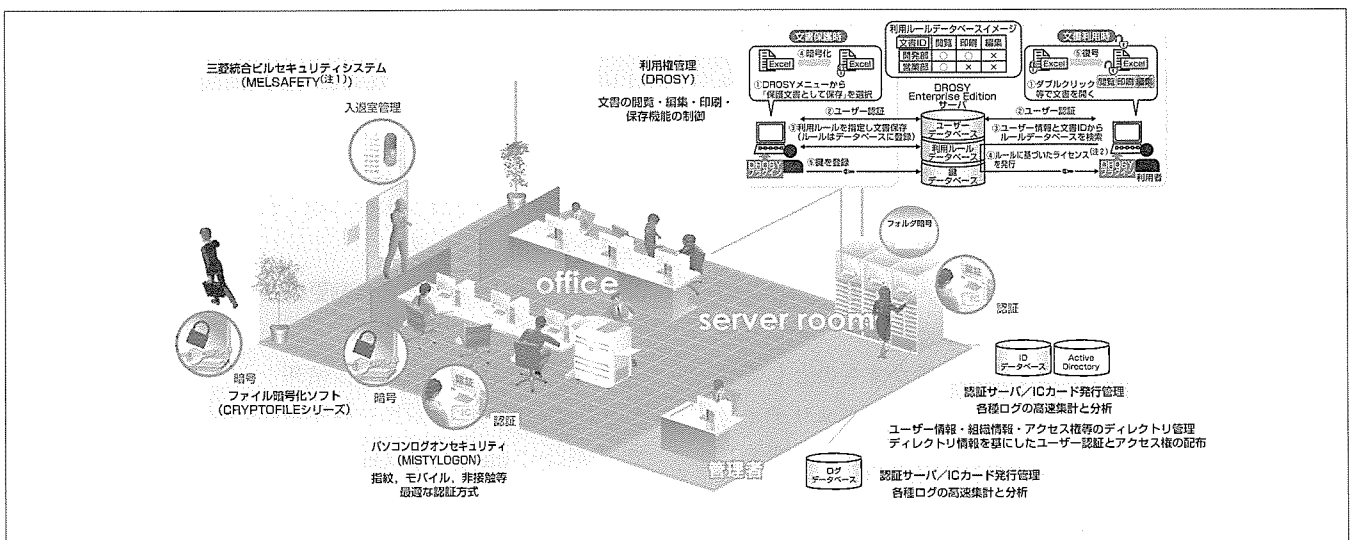
独自管理していたユーザー情報を“Active Directory^(注3)”で一元管理することができ、これまではファイルを個別に暗号化する必要があったが、ファイルサーバ内のファイルを自動で暗号化することができるようにした。

企業において情報セキュリティ管理は事業上で不可欠になっており、情報セキュリティ運用は継続性と実効性が重要である。MDISは、今後も更に使いやすく、運用しやすい情報セキュリティ製品の提供に向け機能強化を継続していく所存である。

(注1) MistyGuard, CRYPTOFILE, MISTYLOGON, MELSAFETYは、三菱電機(株)の登録商標である。

(注2) DROSYは、三菱電機インフォメーションシステムズ(株)の登録商標である。

(注3) Active Directoryは、米国Microsoft Corp.の米国及びその他の国における登録商標である。



MistyGuardソリューションの全体概要

オフィスに入室してパソコンにログオンしてから退出するまでと、退出後の情報セキュリティを確保する。

1. ま え が き

個人情報保護法施行によって、企業は自らが保有する個人情報に対する管理責任を重く受け止め、個人情報を保護する自衛策を導入している。2005年にはP2Pファイル交換ソフトウェア経由で企業の機密情報が流出するという企業の事業継続性を脅かすほどの事故が多発して社会問題となったこともあり、ほとんどの企業は何らかの情報セキュリティ対策を導入していると言われている。

これまで情報セキュリティは特別に機密性の高い情報に対してだけ必要なものとされてきたが、技術の進展と社会環境の変化によって、企業では当たり前に必要なものとして位置付けられ始めている。

このような背景において、MDISでは、情報セキュリティツールだけでなく、組織・個人としての使いやすさを目指したMistyGuardソリューションを提供している。

本稿では、“軽快な運用(利用)”を実現するMistyGuardソリューションについて述べる。

2. 企業の情報セキュリティ対策の課題

2.1 情報セキュリティ対策 I (漏えい防止)

それぞれの企業が実施している情報セキュリティ対策の内容は様々であるが、ほとんどの企業はまずパソコンのハードディスクやファイルを暗号化する対策を実施した。これは出張などで持ち出したパソコンやUSBメモリなどの媒体が盗難や紛失にあっても中の情報が漏えいしないための対策である。また、実際に事故が発生した場合を想定し、データアクセスなどの操作を履歴として残すツールや、パソコンからデータの書き出しを禁止するツールを導入した企業も少なくない。

2.2 情報セキュリティ対策 II (IT統制)

個人情報保護法施行後に発生した漏えい事故では、ファイル交換ソフトウェアを経由してパソコン内の情報が漏えいするというものが目立って報道された。技術的にはファイル交換ソフトウェアを媒介してパソコンがウイルスに感染したことが原因となり、情報セキュリティ対策として、ハードディスクを暗号化するツールを入れるだけではこのような事故は防げないことが明白となった。

これらの事故は企業の事業継続性を脅かすものとして受け止められ、それぞれの企業において情報セキュリティ対策は“情報システム”としての対策にとどまらず、企業としての統制の一部(IT統制)として取り組まれている。

ファイル交換ソフトウェア事故の対策例を下記に示す。

- パソコンの業務用途外使用禁止
- 利用禁止ソフトウェアの指定
- Windows^(注3) アップデートの義務化(脆弱(ぜいじゃく)性抑制)

- ウイルスチェックパターンアップデートの義務化(脆弱性抑制)

- パソコン/媒体の持ち出し許可制度への移行

2.3 情報セキュリティ運用の課題

情報セキュリティ対策は実際の運用では無理や無駄が含まれていることも多く、業務効率よりも“安全”を優先させた結果、業務上支障が生じかねない例もある。

例えば、利用者はパソコンの起動・終了時にいつもデータの暗号化処理で10分間待たされたり、パソコンのログオン時に手帳を見ながら覚えられないほど長いパスワードを入力したりしている。

また、情報セキュリティ事故発生時のリスクは利用者側にも責任分担が大きくなっている。例えば、利用者がUSBメモリでデータを社外に持ち出す場合、利用者は情報漏えいにかかわる宣誓書(覚書)にサインをし、適正な管理手続き(例えば上長承認)を経ることになるが、利用者が安心してデータを持ち出すためには情報セキュリティツールによる十分な保護が必要である。一方、管理者側のコントロールも容易ではない。手続きを用意し、規制を強化してもすべての利用者にルールを守らせることは困難である。利用者の情報セキュリティ対策に対する継続的な啓蒙も重要なことであるが、目の前の情報セキュリティリスクを回避するためには情報セキュリティツールが必要となる。

結果的に、安全・安心のために情報セキュリティツールの導入は欠かせないが、その情報セキュリティツールは利用者及び管理者が運用しやすいものでなければならない。

3. 軽快に使えるMistyGuardソリューション

前章に述べた課題を解決するため、MistyGuardソリューションでは、情報セキュリティ対策をより分かりやすく簡単にし、利用者の負担を軽減させる情報セキュリティソリューションを提供している。例えば、パソコン上のセキュリティ設定を更新することができたり、指紋照合装置付きUSBフラッシュメモリを活用することで、USBメモリ上のデータとパソコン本体の両方のセキュリティ管理等の容易化を実現している。

3.1 セキュリティ設定を自動更新できる暗号化ソフトウェア“CRYPTOFILE PLUS”

CRYPTOFILE PLUSは、情報セキュリティ対策の基本とされているパソコンのデータを暗号化するソフトウェアで、MistyGuardソリューションの核をなす製品である。パソコンの起動及び終了時にハードディスクを丸ごと暗号化及び復号する他の製品と異なり、ハードディスクへの書き込み及び読み出し時に逐次処理するCRYPTOFILE PLUSは、ユーザーをパソコンの起動及び終了時に10分も

(注3) Windowsは、米国Microsoft Corp.の米国及びその他の国における登録商標である。

待たせることはない。さらに、リムーバブルディスクへの書き出しを禁止したり、ファイル操作の履歴を記録したりすることもできる。

CRYPTOFILE PLUSを導入した後に暗号化やリムーバブルディスクアクセスに関するセキュリティ設定(ポリシー)を変更する場合、前バージョンまではCRYPTOFILE PLUSの再インストール及び既に暗号化済みのファイルの復号が必要だったが、今回、ポリシー更新ファイルを作成してサーバから配布するだけで、各パソコン上のセキュリティ設定を自動更新できるようにした(図1)。ポリシー更新ファイルは改ざん防止のためにCRYPTOFILE PLUSの導入時に生成されたポリシーグループ鍵(かぎ)で暗号化されており、ユーザーによるセキュリティ設定の改変を防止している。

3.2 指紋照合装置付きUSBフラッシュメモリでデータとパソコンを守るパソコンログオンセキュリティ“MISTYLOGON Lite”

パソコンログオンセキュリティMISTYLOGONのこれまでのバージョンでは、管理用サーバを必要としていたため、簡単に導入したい顧客のニーズにはこたえられなかった。

MISTYLOGON Liteでは、管理用サーバを使用せずに、指紋照合装置付きUSBフラッシュメモリでパソコンへログオンすることができるよう、管理機能をパソコン内に実装している。あらかじめログオン情報(ID・パスワード)と指紋データを関連付けることで、ID・パスワードを入力することなく、指紋照合することでパソコンに自動ログオンできるようにした(図2)。これによって、ユーザーは、覚えきれないほど長いパスワードを手帳を見ながら間違わないように慎重に入力するようなことは必要なくなる。また、指紋データは2指登録できるため、指先のコンディションによる照合エラーに対応することを可能とした。

また、定期的にログオンパスワードを変更する必要がある場合は、指紋照合によって管理者ツールを実行し、関連付けたログオン情報を更新することで対応できる。

MISTYLOGON Liteの指紋照合装置付きUSBフラッシュメモリは、データを安全に持ち出すための媒体としても

活用することができる。指紋照合でログインすることでUSBフラッシュメモリへのデータアクセス(書き込み、読み出し)が可能となるため、安全なデータの持ち運びも実現することができる。

また、ログオン履歴をログに記録し、ログを収集するオプション製品“MISSIONLOG”と組み合わせて他のMistyGuardソリューションと統合化されたログを参照することもできる。

MISTYLOGONには、指紋照合装置付きUSBフラッシュメモリ以外にも、ICカード(接触型・非接触型)や指紋照合装置でログオンする製品もラインアップしている(図3)。

3.3 企業機密情報管理“DROSY Enterprise Edition”

企業内の機密情報を安全に共有するためのソリューションとしてDROSY Enterprise Editionを提供しており、DROSY機能で暗号化された機密文書に対して利用ユーザーと操作を制限(利用権保護)することができる。利用権保護された文書は常に暗号化された状態にあるため、万が一ファイル交換ソフトウェアなどの不正使用によって外部に流出しても機密を保持することができる。

これまでのバージョンでは、導入及び運用に当たって大きく2つの課題があった。一つ目の課題は文書の利用権保護方法についてであり、これまで一つ一つの文書を指定してDROSY機能で利用権保護していたために手間がかかっていた。これに対し今回のバージョンでは、DROSYサーバ上の利用権保護用フォルダを使用して、そのフォルダに保存された文書を自動的に利用権保護することができる

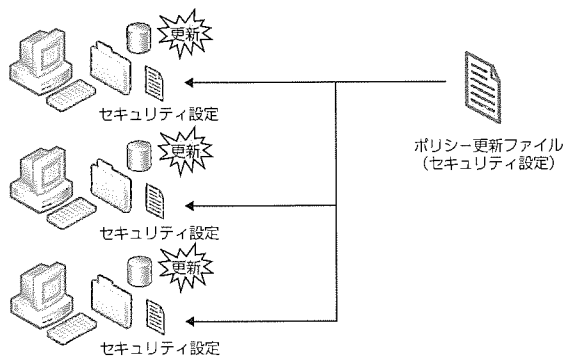


図1. CRYPTOFILE PLUSのポリシー更新

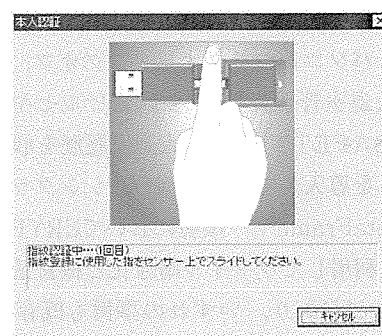


図2. MISTYLOGON Liteの指紋照合画面

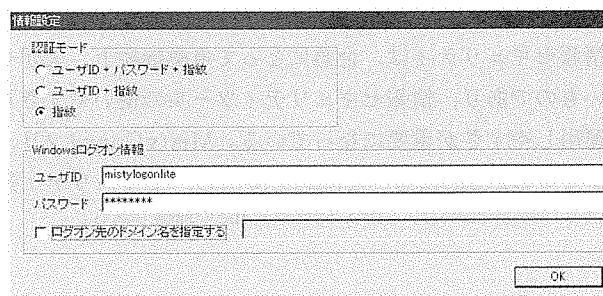


図3. MISTYLOGON Liteのログオン情報連携

(フォルダ自動保護機能)。これによって、文書を利用権保護する手間を大幅に削減することができた。この利用権保護用フォルダはサブフォルダにも対応しており、そのまま共有フォルダとしても使用できる(図4)。

二つ目の課題はユーザー情報管理についてであり、これまでのバージョンではDROSY独自でユーザーを管理する必要があった。これに対し今回のバージョンでは、Active Directoryと連携してユーザー情報を一元管理することができる“Active Directory連携アダプタ”を開発した。これによって、Windowsのログオンユーザー=DROSYの利用ユーザーとして管理でき、ユーザー認証も統合化されるため、管理者はユーザー管理の負担を軽減できる。さらに、Active Directoryのユーザーグループもそのまま取り込むことができるだけでなく、ユーザーグループに“組織階層”を表す追加情報を定義することで階層化(最大10階層)された組織として取り込む機能を実現している。

4. MistyGuardソリューションの事例

以上に述べた3つの製品を含め、MistyGuardソリューションの事例を述べる。

MISTYLOGON Liteの指紋照合装置付きUSBフラッシュメモリでパソコンにログオンすることで、自動的にCRYPTOFILE PLUS, DROSY, Active Directoryにもログオンしている事例を図5に示す。この事例ではすべてのユーザー管理をActive Directoryで一元管理しており、共有ファイルサーバはドメインユーザー管理によってアクセス制御され、一部のファイルはDROSYによって利用権が保護されている(フォルダ自動保護機能は未使用)。

そのほか、パソコンのログオン・ログオフ、ファイル操作履歴及び入退室管理装置(三菱統合ビルセキュリティシステムMELSAFETY)からの入退室履歴を収集するログ管理システムを導入している事例や、シンクライアントを使用した“MetaFrame^(注4)”環境においてCRYPTOFILE及びDROSYを利用してファイル暗号化と機密情報共有をしている事例などがあり、いずれの事例も既存システムとMistyGuardソリューションが連携してより使いやすく運用しやすいシステムを提供している。

5. む す び

情報セキュリティは、企業にとって事業継続上、欠かせないものであり、情報セキュリティツールの使いやすさ及び運用しやすさが重要になっている。MistyGuardソリューションは2.3節に述べた課題を解決し、セキュリティ運

(注4) MetaFrameは、Citrix Systems, Incの商標である。

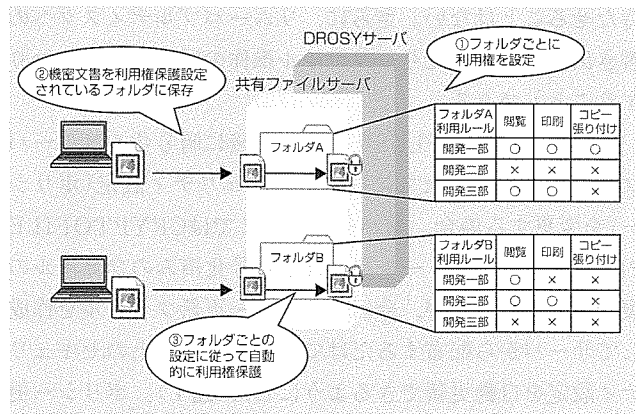


図4. DROSY Enterprise Editionのサーバフォルダ監視による機密情報の自動変換

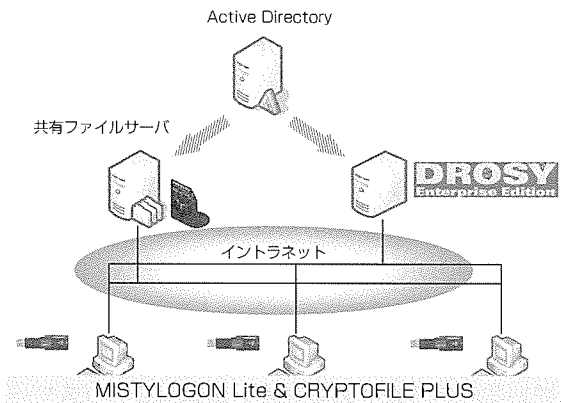


図5. MistyGuardソリューションの利用事例

用を軽快にすることができる。

さらに、今後は情報セキュリティ対策の継続性と実効性が重要になってくると考えており、MDISではMistyGuardソリューションをより一層使いやすく、運用しやすいものにするとともに、情報セキュリティによるIT統制機能の強化を図っていく所存である。

参考文献

- (1) 経済産業省：“企業における情報セキュリティガバナンスのあり方に関する研究会報告書” (2005)
- (2) 青木隆之, ほか：個人情報保護法, e文書法にも対応可能なトータルセキュリティソリューション, 三菱電機技報, 79, No.4, 279~284 (2005)
- (3) 森口 修, ほか：機密文書の安全な公開を実現する電子文書ライフサイクルマネジメントソリューション, 三菱電機技報, 80, No.4, 285~288 (2006)

多種多様なログの統合管理を実現する “LogAuditor Enterprise”

郡 光則*
森田 登**
藤村 隆**

“LogAuditor Enterprise” : Integrated Management System for Various Log Data

Mitsunori Kori, Noboru Morita, Takashi Fujimura

要 旨

近年、企業内の内部統制やセキュリティ管理に対する関心の高まりを背景に、様々な情報システムが生成する大量のログを証拠保全のために蓄積保存するようになってきた。従来、これらのログは個々の情報システムごとに管理されることが多かったが、ログの種類が増加に伴い、これらのログを統合的に管理し、管理コストの低減や原因分析の効率化を図る必要性が高まっている。一方、汎用のRDB (Relational DataBase)を利用する従来のログ管理では、形式の異なるログの一元的な取扱い、蓄積・検索速度、ストレージコストなどの点に課題があった。

三菱電機インフォメーションテクノロジー(株)(MDIT)の内部統制推進ソリューション“LogAuditor Enterprise^(注1)”は、大量に発生する任意形式ログの収集・蓄積・分析を可能とするための統合的なログ管理機能を提供するソフトウェア製品である。

LogAuditor Enterpriseは、以下の三菱電機独自の高速処理技術を活用して大規模なログの高速処理を実現した。

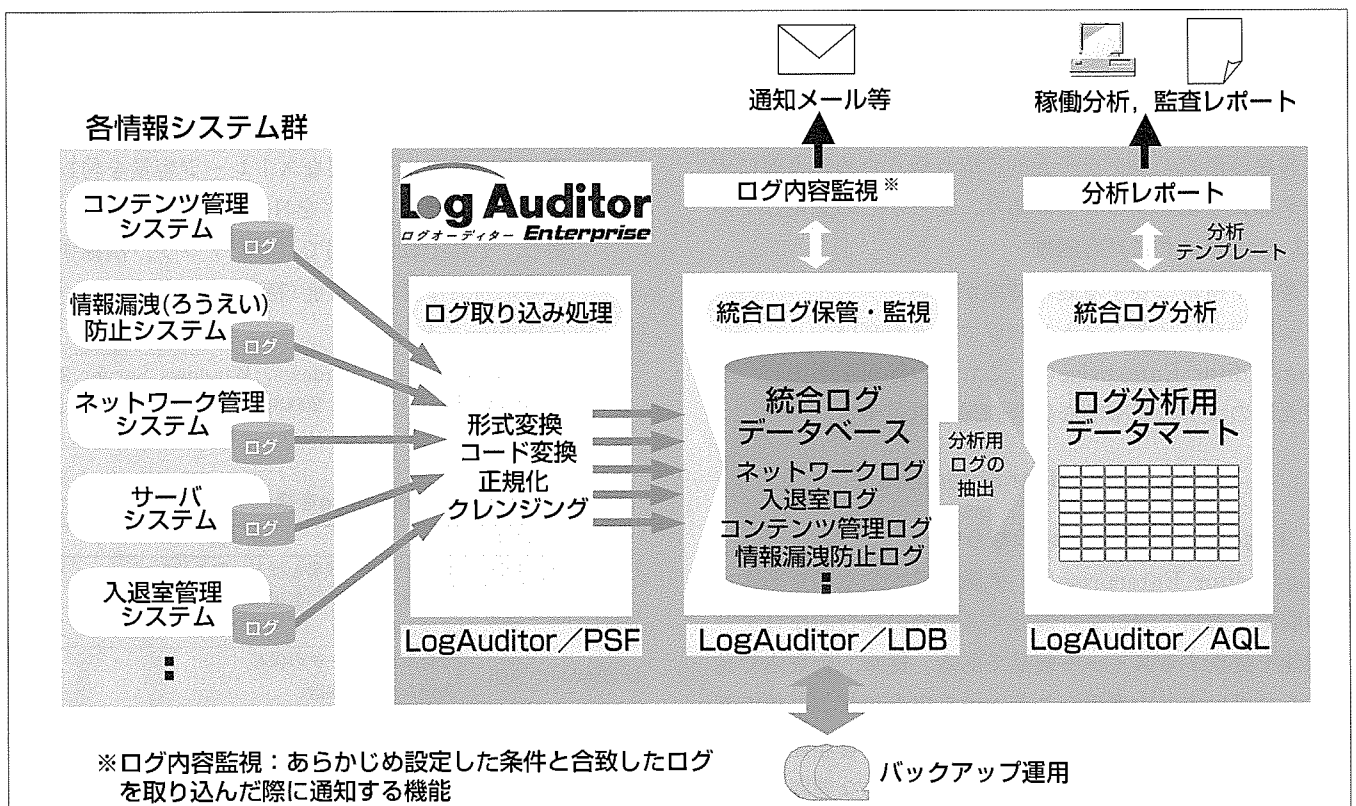
- (1) データ量を1/10以下に削減し、ストレージコスト低減と高速化を実現するデータ圧縮技術
- (2) データ規模に応じた処理速度とスケーラビリティの高いシステム構成を実現する並列処理技術
- (3) データ蓄積後のログ形式判別や索引を使用しない検索を高速に行う高速文字列照合技術

また、LogAuditor Enterpriseを活用したソリューションとして提供する“分析テンプレート”により、各種のログを統合した監査レポートを出力することができる。

今後は、ログの大規模化と多様化が進むと予想されるため、更なるスケーラビリティの拡大及び分析テンプレートの充実化を図っていく予定である。

(注1) LogAuditorは、三菱電機インフォメーションテクノロジー(株)の登録商標である。

特集
I



Log Auditor Enterpriseのシステム構成

Log Auditor Enterpriseは、ログの取り込みを行うLog Auditor/PSF、統合的にログを保管・監視するLog Auditor/LDB、統合的なログの分析エンジンであるLog Auditor/AQLから構成される。また、分析フロントエンドとなるMicrosoft Excelアドインを利用できる分析テンプレートが提供される。

1. ま え が き

近年の企業内の内部統制やセキュリティ管理に対する関心の高まりを背景に、コンテンツ管理システム、情報漏洩防止システム、ネットワーク管理システムなど様々な情報システムから生成される利用履歴(ログ)が証拠保全のために蓄積・保存されるようになってきた⁽¹⁾。蓄積されるログの量は年間数十テラバイトに及ぶ事例も見られる。従来、これらのログは個々の情報システムごとに管理されることが多かったが、ログの種類やデータ量の増加に伴い、これらのログの統合的な管理により、管理コストの低減や原因分析の効率化を図る必要性が高まっている。

MDITでは、企業内の情報システムで採取されるログを証跡として収集・蓄積し、分析する内部統制推進ソリューションLogAuditor Enterpriseを提供し、多種多様なログの統合管理を実現した。

本稿では、従来のログ管理の課題と、LogAuditor Enterpriseによる解決策、及びそれを支える高速処理技術について述べ、併せて、LogAuditor Enterpriseを活用したテンプレートについても述べる。

2. ログ管理の課題

従来のログ管理では、汎用のRDBを利用することが多かった。しかし、OLTP(On-Line Transaction Processing)などを主対象として発達してきたRDBは、様々な形式を持ち、長大なデータを含むことの多いログの効率的処理には必ずしも適していない⁽²⁾。このため、ログの種類や量の増大に伴い、以下の問題が見られるようになってきた。

- (1) 異なる形式のログを一元的に取り扱うために事前にデータ形式を統一する必要がある、あらかじめ想定していない形式のログに対応困難
- (2) 蓄積や検索に要する処理時間が長い
- (3) 長期保存に必要なストレージコストが高い

LogAuditor Enterpriseは、これらの課題を解決し、多様で大量のログの効率的な統合管理を実現する。

3. LogAuditor Enterprise

3.1 LogAuditor Enterpriseのねらい

LogAuditor Enterpriseは、大量に発生する任意形式ログの収集・蓄積・分析を可能とするための統合的なログ管理機能を提供するスイート製品である。従来、企業内で発生するログは各々の専用システムから出力され、単体で蓄積・管理が行われており、それらを統合して管理運用することは前述のログ管理の課題で述べた技術的な課題もあり難しかった。そのため、複数のログを横断的に分析し企業内で発生しているイベント、機器の操作などを総合的に把握及び分析することは困難で、蓄積されたログを必ずしも

十分に活用できるとは言い難かった。LogAuditor Enterpriseは、この課題を解決するソリューション製品である。

3.2 製品の構成

LogAuditor Enterpriseは、主にログの取り込みを行うLogAuditor/PSF(Power Staging Facility)、統合的にログを保管・監視するLogAuditor/LDB(Log DataBase)、統合的なログの分析エンジンであるLogAuditor/AQL(Analytical Query Language)から構成され、さらに、分析フロントエンドとなるMicrosoft Excel^(注2)アドインが提供される。それらの機能、動作環境について表1、表2に示す。

(1) LogAuditor/PSF

LogAuditor/PSFは、企業内に存在する様々なログデータを収集し加工するシステムであり、以下の特長を持っている。

- きめ細かいデータの加工、編集機能
- 高い生産性・保守性
- サポートされるデータソースは、各種ログが格納された主要RDB又はCSV(Comma Separated Value)などのフラットファイル

(2) LogAuditor/LDB

LogAuditor/LDBは上記の課題を解決する新しい概念のデータベース管理システムであり⁽³⁾、以下の特長を持っている。

- ログをその形式によらず完全に復元可能な形で蓄積保存。事前にログ形式の特定は不要
- テラバイト超の大規模ログにも対応可能な高速蓄積と正規表現指定による高速検索保持
- データ圧縮により必要なストレージ容量を約1/10以下に削減。また、ログを日単位などの“範囲”に分割し、それぞれの範囲でバックアップ、削除するなど時系列的な管理が可能(特許出願中)

(3) LogAuditor/AQL

(注2) Microsoft, Excel, Windows, Windows Server 2003, Windows XP, Windows 2000は、米国Microsoft社の登録商標である。

表1. LogAuditor Enterpriseを構成するコンポーネント

コンポーネント	機能
LogAuditor/PSF	ログデータの収集と加工、取り込み
LogAuditor/LDB	統合ログデータの蓄積保管・監視 高速な検索
LogAuditor/AQL	分析用ログデータの保存 高速な検索・集計
分析フロントエンド	分析テンプレートなどによる定型レポート 非定型分析レポート

表2. LogAuditor Enterpriseの動作環境

サーバ	Microsoft Windows ^(注2) Server 2003 ^(注2)
クライアント	Microsoft Windows XP ^(注2) Professional
	Microsoft Windows 2000 ^(注2) Professional

LogAuditor/AQLはデータ集計・分析に適したデータベース管理システムであり、以下の特長を持っている。

- 集計・分析に適した構造化されたデータとしてログを保存
- 高速なデータ検索・集計
- データ圧縮による必要ストレージ容量の削減
- 標準SQL (Structured Query Language) に準拠した柔軟なアクセスインタフェース

(4) 分析フロントエンド

LogAuditor/AQLの分析用フロントエンドとして表計算ツールであるMicrosoft Excelから直接アクセスし、分析レポートの作成を可能とするExcelアドインツールを提供し、以下の特長を持っている。

- 定型レポートの雛形(ひながた)となる分析用テンプレートの作成、利用が可能
- 柔軟な非定型分析、ウィザード形式での容易な操作
- 使い慣れたExcelからシームレスに利用可能、集計表(ピボットテーブル)を自動生成
- 集計値から明細の分析データにさかのぼるドリルスルー機能
- 原始ログデータとも連携可能なアプリケーションやマクロの利用

4. LogAuditor Enterpriseの高速処理技術

LogAuditor/LDBとLogAuditor/AQLは、いずれも当社独自の大規模データ高速処理アーキテクチャSISA (Scalable Intelligent Storage Architecture) に基づき大規模ログの高速処理を実現した。以下に、その主要技術について示す。

4.1 データ圧縮技術

LogAuditor/LDB, LogAuditor/AQLは、ログを自動的に圧縮して蓄積することにより、必要なストレージ容量を約1/10以下に削減する。また、データ圧縮によりストレージ入出力が削減されるため、蓄積・検索速度も向上する。

図1に、LogAuditor/LDBにパソコン操作ログ(レコード長約700バイト)を格納した場合のデータ量削減効果の一例を示す。この例では、RDBを使用した場合と比較して、必要なストレージ容量が約1/23に削減されている。

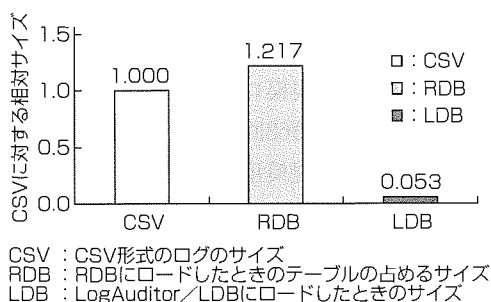


図1. データ圧縮によるデータ量比較(LogAuditor/LDB)

4.2 並列処理技術

LogAuditor/LDB, LogAuditor/AQLでは、圧縮、伸張、検索処理を複数のプロセッサにより並列処理し、プロセッサ数に応じた処理速度の向上を実現する。また、データを複数のストレージに自動的に分散配置し、並列に入出力を行う。これにより、ログのデータ量に応じたプロセッサやストレージを用意することによって、スケーラビリティの高いシステムを提供できる。図2に、パソコン操作ログを対象とするLogAuditor/LDBのプロセッサ数ごとの全件検索速度性能の一例を示す。

4.3 高速文字列照合技術

LogAuditor/LDBは、蓄積時にログの形式を指定する代わりに、蓄積後にログ形式を判別しながらログを抽出可能であるという特長を持っている。しかし、従来の文字列照合方式では、ログの形式判別に必要な複雑な照合処理に十分な速度が得られなかった。LogAuditor/LDBでは、当社独自のsDFA (size-reduced Deterministic Finite Automaton) 方式⁽⁴⁾ (特許出願中)により条件式規模によらずほぼ1億文字/秒の高速処理を実現し、この問題を解決した(図3)。

一般にデータベース検索の高速化には索引を利用することが多いが、ログ管理では、蓄積速度の低下やストレージ容量の増大が問題になる。LogAuditor/LDBでは、高速文字列照合技術により、蓄積速度、ストレージ容量と検索速度の両立を図った。

5. 統合ログ管理ソリューション活用例

MDITでは、LogAuditor Enterpriseを活用したソリューションとして、企業内の業務フロー実行ログ、パソコン操作ログ、ファイルサーバアクセスログなどを統合管理した結果から、内部統制を目的とした監査レポートを出力す

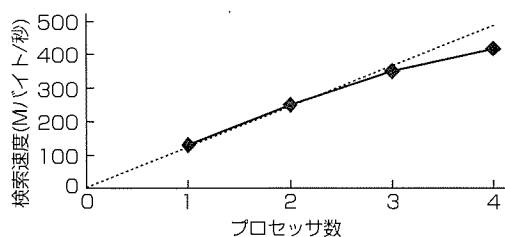


図2. ログの全件検索速度性能(LogAuditor/LDB)

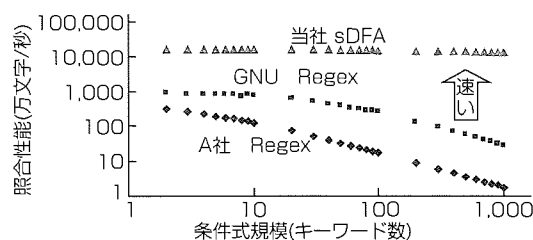


図3. 文字列照合速度性能の比較

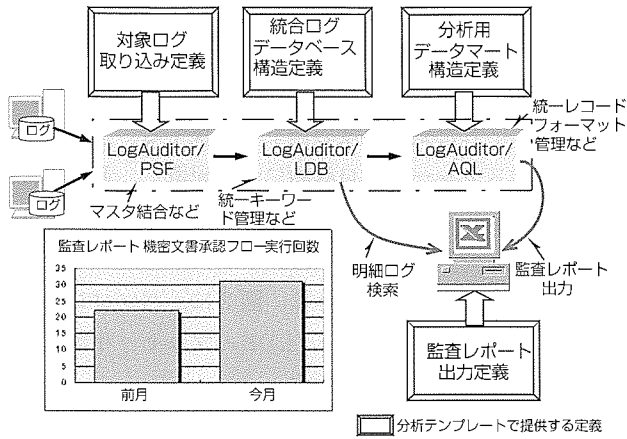


図4. 分析テンプレートの構成イメージ

る“分析テンプレート”を提供している(図4)。分析テンプレートは、対象とする製品のログ仕様ごとに、統合ログデータベースの構造、ログ分析用データマートの構造、ログの取り込み形式を定義することで、これらを統合したログからMicrosoft Excel形式の監視レポートを出力する。

通常、ログは文字列形式によりシステムで発生した事象を記録しており、その膨大な文字列情報からいかなる行為や出来事が起きているのかを人間が直感的に把握するのは困難である。例えば、機密ファイルへのアクセス件数が、前月と比較して増えているのか、また、その傾向は業務フローの実行状況と関係があるのかなどは、ファイルサーバや業務アプリケーションのログ(文字列情報)参照だけでは解析が非常に困難である。この問題を解決するために無形のログを表やグラフ形式に可視化して報告する機能が監視レポートであり、その一例を図5に示す。機密ファイルのアクセスが利用者の業務状況に合致しているかが一目で分かる例を示しており、仮に異常なアクセス件数を示した場合には、適切な業務以外でのアクセスが多すぎると判断でき、セキュリティ管理策の検証や見直しなどに活用できる。

このように、異なるシステムのログであったものを同じ視点で集計・参照することで、複数システムの利用状況を統合的に管理することが可能になる。さらに、LogAuditor Enterpriseでは、詳細な原因追求のために不可欠な“ログ明細にさかのぼった検索”を、監視レポートの該当箇所から超高速に実行することが可能である(図5のログ明細表示)。

上記の内部統制での活用例のほか、統合ログ管理ソリューションは、表3に示すような情報セキュリティ管理を始めとする様々な分野での活用が可能であり、今後、分析テンプレートの充実化を推進する。

6. む す び

多種多様なログの統合管理を実現するLogAuditor Enterpriseについて述べた。今後は、ログの大規模化と多

日付	時間	曜日	操作	ファイル名	ユーザ名
2005/8/6	11:23:16	月	ファイル読み込み	〇〇社PJ業務録	fujitaka
2005/8/6	11:43:17	月	ファイル読み込み	〇〇社PJ見積書	sasaki
2005/8/6	13:20:37	月	ファイル読み込み	〇〇社PJ工程表	morita
2005/8/6	13:23:18	月	ファイル読み込み	価格表	koori

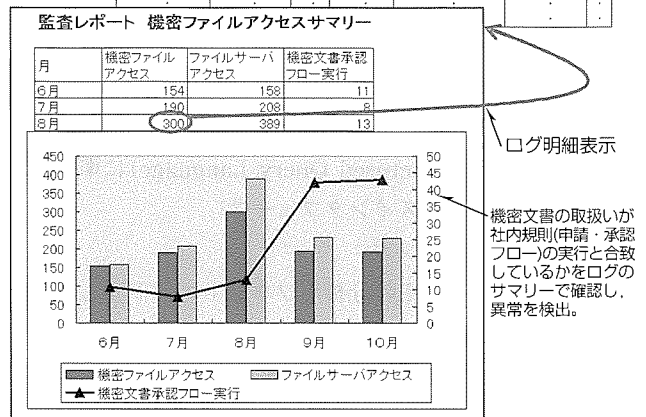


図5. 監視レポート例

表3. 統合ログ管理活用の対象業務例

対象業務	ログの種類	活用例
情報セキュリティ	・ パソコン操作ログ ・ サーバアクセスログ ・ データベースアクセスログ ・ 電子メールログ ・ 入退室管理ログ ・ ファイル暗号化ログ ・ Webアクセスログ	利用者権限に従った社内情報使用の状況把握→セキュリティポリシーの見直し(PDCAサイクル)
内部統制	・ コンテンツ管理ログ ・ パソコン操作ログ ・ サーバアクセスログ	業務フローの実行と合わせた現場での情報利用の確認→監査資料の出力
情報インフラ管理	・ ネットワークログ ・ 電子メールログ ・ Webアクセスログ ・ サーバアクセスログ ・ 複合機ログ	ネットワーク負荷状況、共有の情報システム機器の稼働状況の確認→情報インフラ整備の最適化
情報システム運用管理	・ ネットワーク機器ログ ・ パソコン操作ログ ・ サーバアクセスログ	情報システム機器の運用状況の確認→機器、ジョブの運用スケジュールの最適化

PDCA: Plan Do Check Action

様化が進むと予想されるため、更なるスケーラビリティの拡大化及び分析テンプレートの充実化を図る予定である。

参 考 文 献

- (1) 内部不正の目撃者, 日経コンピュータ2006/5/1号, No.651, 40~55 (2006)
- (2) Sah, A.: A New Architecture for Managing Enterprise Log Data, Proc. of LISA 2002, 121~132 (2002)
- (3) 中村隆顕, ほか: 大規模ログデータベースの実現, 情報処理学会全国大会第68回, 1D-2 (2006)
- (4) 中村隆顕, ほか: 大規模正規表現の高速照合方式, 情報処理学会全国大会第67回, 4F-5 (2005)
- (5) 藤村 隆, ほか: 情報のリスク管理・内部統制を支援するコンプライアンス推進ソリューション, 三菱電機技報, 80, No.4, 281~284 (2006)

統合セキュリティ管理サービス

太田 潔* 榊原裕之**
 田中 朗* 平井規郎**
 藤井誠司**

MIND Integrated Security Management Service

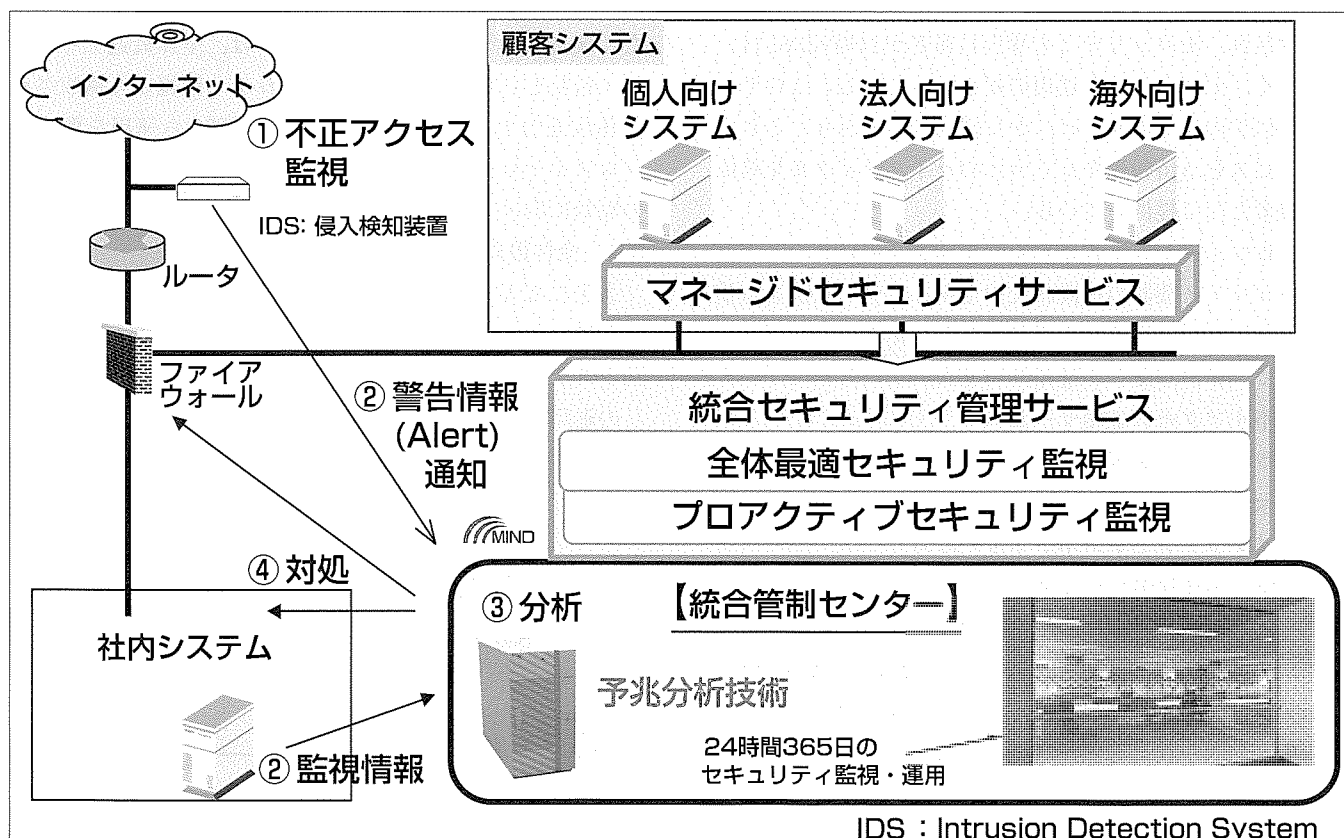
Kiyoshi Ohta, Akira Tanaka, Seiji Fujii, Hiroyuki Sakakibara, Norio Hirai

要 旨

三菱電機情報ネットワーク㈱(ＭＩＮＤ)では、情報セキュリティビジネスとして、1998年からセキュリティ運用監視サービスを提供しており、トータルなセキュリティソリューションとして“MINDマネージドセキュリティサービス”を提供している。MINDは、2003年に、“情報セキュリティマネジメントシステムISMS(Information Security Management System)”適合性評価制度及びBS7799の認証を三菱電機グループでは初めて取得し、セキュリティサービスを提供する企業として、積極的に情報セキュリティビジネスに取り組んできた。

本稿では、監視対象システムの構築から運用、監視、対

応、セキュリティ情報収集・分析までのセキュリティサービスを提供しているMINDマネージドセキュリティサービスへの取り組みについて述べる。また、セキュリティ監視サービスの更なる質の向上を目指して、2005年度から新たに開始した“統合セキュリティ管理サービス”についても述べる。統合セキュリティ管理サービスは、全体最適セキュリティ監視とプロアクティブセキュリティ監視から構成される。特に、プロアクティブセキュリティ監視については、情報セキュリティにおける未知の不正アクセス検知及びその対策実現のために三菱電機㈱ 情報技術総合研究所と共同で開発を進めている予兆分析システムについても述べる。



統合セキュリティ管理サービス

MINDマネージドセキュリティサービスでは、①IDSによるインターネット及び社内システムの不正アクセスの監視、②統合管制センターへの警告情報通知、③統合管制センターでの分析、④対処を実施している。新たな全体最適セキュリティ監視及びプロアクティブセキュリティ監視機能の提供により、更なる監視サービスの質の向上を目指している。

要な過去のネットワーク監視データを逐次削除しながらデータ分析する機能を新規に開発し、その機能を組み込むことで、検知性能の低下を防止した。

(3) 検証結果

上記のような特長を持つDynamicSVDの有効性を検証するために、以下のネットワーク監視データによりDynamicSVDの機能検証を行い、未知の攻撃を検知できることを検証した。

- (a) 米国リンカーン Laboratory IDS 評価データ
- (b) JPCERT/CC(Coordination Center)の定点観測データ
- (c) MIND 定点観測データ

図4は、上記(c)のMINDの定点観測データを分析した結果である。セキュリティ監視の対象となっているネットワークに設置した定点観測センサが、ある場所に不正にアクセスしようとする試みが何回あったかを60分ごとに記録した例である。例えば、IDS等で用いられるしきい値方式では、あらかじめ設定したしきい値を決められた回数超えた場合(図では、連続して3回しきい値を超えた場合を異常と判定)に異常と判断する。未知の攻撃に対して、最適なしきい値を設定することは困難である。DynamicSVDを用いて通常の通信状況との違いを統合的に分析した結果、しきい値方式による検知と比較して約3分の1の時間で検知することができた。

4.2 今後の展開

顧客はセキュリティ監視サービスに対して、単に検知することではなく、早期に未知の攻撃を検知して、早期に対策が実施されることを求めている。以下では、想定される課題を明確化するとともに、それらの課題の解決手段として開発を進めている機能について述べる。

(1) 早期検知

早期の検知を実現するためには、セキュリティ監視システムからオンラインでログを取得して分析する必要がある。統合セキュリティ管理サービスでは、SIMによってファイアウォール及びIDSからログを収集し、分析する環境を整備している。予兆分析システムを統合セキュリティ管理サービスで活用するためには、SIMと連携し、オンラインでログを入手し、未知の攻撃の早期検知を実現する必要がある。しかし、SIMに蓄積されるログは膨大であるため、セキュリティ監視システムへの運用を妨げずにリアルタイムに警告情報を入手するSIM連携機能の開発を実施している。

(2) 早期検知の有効活用

未知の攻撃を検知するためには、1種類のネットワーク監視データを分析していても検知性能は向上しない。そのためには、様々なネットワーク監視データを適切な設定で分析することが必要である。また、様々なネットワーク監視データの分析結果をセキュリティ監視サービスの分析担当者が再度総合的に分析していたのでは、早急に対策をと

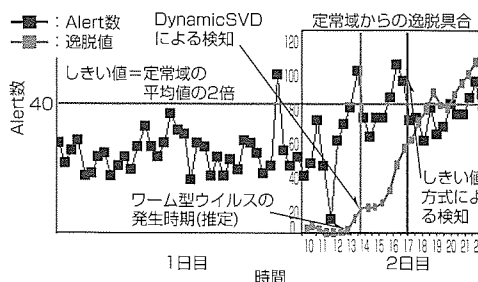


図4. 不正アクセスの検知方法による検知時間の差

ることができない。ここでは、統合判定機能に判定精度が重要な課題となる。現在、判定精度の高い統合判定アルゴリズムの研究開発を行っており、このアルゴリズムを使用して、予兆分析結果を統合的に判定し、早期対策を実現するための情報(攻撃の種別、攻撃の確からしさ(確度)、攻撃に関係する送信元アドレスやアプリケーションの特定)を提供する統合判定機能を開発する予定である。

(3) 対策方法の特定

早期対策を実現するためには、異常が起きたことが分かるだけでなく、その異常の原因及びその原因を解消するための対策情報が必要である。また、早期検知から早期対策までの時間を短縮化するためには、人手による対策だけではなく、自動的に対策を実施できる手段も必要である。そこで、統合判定機能が提供する情報及び公開されている脆弱性情報から監視対象に設置されたセキュリティ装置で対策を実施する早期自動対策機能の開発も進めている。

5. む す び

本稿では、MINDで展開してきたMINDマネージドセキュリティサービスについて概観した。そして、2005年度から開始した統合セキュリティ管理サービスについて概要を述べ、現在、取り組んでいる予兆分析システムについて述べた。現在、上記の機能を開発するとともに、実用化に向けて、実ネットワーク上でDynamicSVDを用いた予兆分析技術の効果を検証する実用化試験を行っている。そして、2007年度から予兆分析システムのサービスの運用開始を目指している。

今後は、顧客満足度の高いセキュリティ監視サービスを実現するために、サービスの最適化及び新たな付加価値の創出にも努力していく所存である。

参考文献

- (1) 榊原裕之, ほか: 定点観測による不正アクセス分析システムの提案, 2006情報処理学会第68回全国大会, 5E-3 (2006)
- (2) 平井規郎, ほか: 定点観測による不正アクセス分析システムの提案-ワーム攻撃による異常検出のためのネットワークログ分析手法, 2006 情報処理学会第68回全国大会, 5E-4 (2006)

電子文書の長期原本性保証を実現する “EVERSIGN”

宮崎一哉*
山中忠和*
田中 学**

EVERSIGN : Long-Term Storage System for Signed Documents

Kazuya Miyazaki, Tadakazu Yamanaka, Manabu Tanaka

要 旨

e-文書法の施行や日本版SOX法(「証券取引法等の一部を改正する法律」及びその整備法)の成立により、文書の真実性及び適正性が強く問われる状況となっている。電子的な文書の真実性及び適正性を確保するためには、電子署名やタイムスタンプが利用される。これらはデジタル署名という公開鍵(かぎ)暗号基盤PKI(Public Key Infrastructure)に基づく技術で構成されるが、この技術は公開鍵証明書が持つ有効期間や失効という仕組みに起因する制約のため、長期間その有効性を維持することができない。

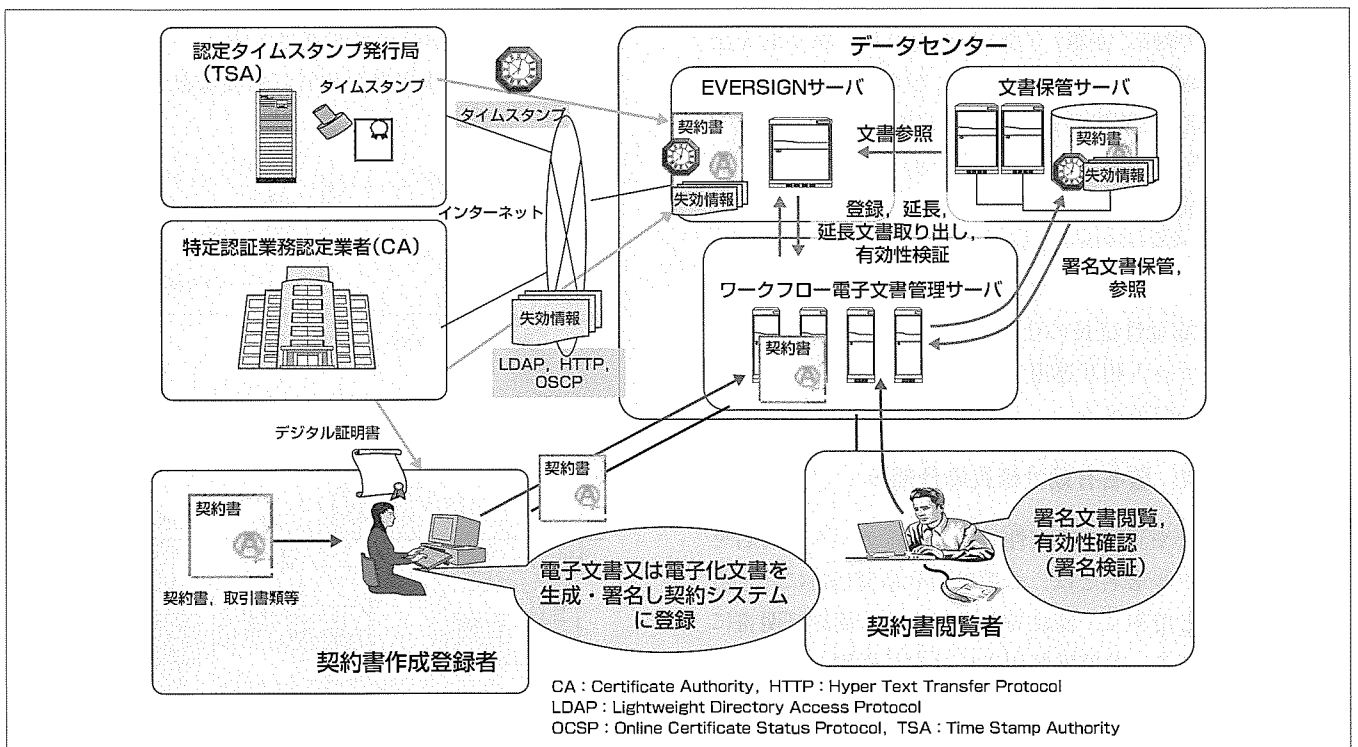
長期署名フォーマットは、デジタル署名の持つこのような制約を解消するための効果的な手段を提供するためのフォーマットである。長期署名フォーマットによるデジタル署名の有効性延長方式は、その構築や検証が複雑であるものの、だれでも有効性を検証できる極めてポータビリティが高い等の優れた特長を持っている。

長期署名フォーマットは、国際的な標準仕様として定義されている。ポータビリティ確認のために、2005年度末には、次世代商取引推進協議会(ECOM)で、標準プロファイルに基づく相互運用性実験が実施された。

“三菱署名有効性延長システムMistyGuard^(注1)“EVERSIGN^(注2)”は、標準の長期署名フォーマットの自動構築や検証機能を提供するサーバシステムであり、上記相互運用性実験において、標準プロファイルへの適合性が確認されている。e-文書法や日本版SOX法に適合するシステムを構成するコンポーネント製品として既に幾つかの電子文書・記録管理システムで採用されており、今後、ますます同分野での貢献が期待される。

(注1) MistyGuardは、三菱電機(株)の登録商標である。

(注2) EVERSIGNは、三菱電機インフォメーションシステムズ(株)の登録商標である。



EVERSIGNを応用した長期保存機能付き電子契約書管理サービス例

電子契約書の真実性確保のためには、電子契約書にデジタル署名を付与した上で送受を行う。最終的に電子契約書を保存する場合、法律で定められた保存期間(例えば7年、10年など)にわたってデジタル署名の有効性を維持する必要がある。EVERSIGNを導入することにより、通常は1~3年で切れる有効性を永続的に維持することが可能となる。

1. ま え が き

2005年4月1日に施行されたe-文書法(「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」及びその整備法)により、原則的にすべての保存義務のある文書を電子的に保存することが許された。これは主に紙文書の保管コストの削減ニーズに端を発するものであったが、電子的文書の活用による業務の効率化や紙文書の削減による資源保護といった積極的な目的にもかなう動きである。

一方、米国におけるエンロンやワールドコムによる会計不祥事を契機に、2002年7月に企業改革法(サーベンス・オクスリー法:SOX法,「Public Company Accounting Reform and Investor Protection Act of 2002:上場企業会計改革及び投資家保護法」が正式名称)が米国で承認され、日本でも日本版SOX法が2006年6月に成立し公布された。

e-文書法では、税務関連文書や医療関連文書等の重要な文書については、電子的保存の要件として“真実性の確保”が挙げられており、真実性の確保のためにデジタル署名及びタイムスタンプを利用することが要求されている。

また、日本版SOX法では、記録の適正性や適切に記録及び保存されることが要件として挙げられているものの、“記録”が電子的なものであるとは限らないこともあり、具体的にそれらの技術の利用が要求されているわけではない。しかし、日本版SOX法では、ITが組織に浸透した現状に即して“ITへの対応”が謳(うた)われており、電子的な記録の適正性確保と保存が要求されることが考えられる。

本稿で述べる“三菱署名有効性延長システムMistyGuard“EVERSIGN””は、標準の長期署名フォーマットに基づいて、電子的な文書や記録の真実性又は適正性を長期にわたって保証することにより、e-文書法や日本版SOX法に適合するシステムを構成するコンポーネント製品である。次章以降、署名有効性延長の仕組み、ECOMで実施した長期署名フォーマット相互運用性実験への参加結果、そして適用事例について述べる。

2. 署名有効性延長の仕組み

電子的な文書や記録の真実性確保には、デジタル署名を用いる。デジタル署名とは、公開鍵暗号基盤PKIにおける電子署名のことであり、認証局の発行する公開鍵証明書に信頼の基点を置く。公開鍵証明書には有効期間や失効という仕組みが存在し、デジタル署名の有効性は公開鍵証明書の有効期間や失効に依存する(図1)。つまり、公開鍵証明書が有効期間を超過し又は失効してしまうと、デジタル署名の有効性も失われる。

これは、公開鍵証明書が有効期間を超えてしまうと、署名用の鍵の漏洩(ろうえい)やアルゴリズムの脆弱(ぜいじ

ゃく)化により署名が偽造される可能性を否定できなくなるためであり、また、失効の場合も同様で、漏洩した鍵により署名が偽造される可能性を否定できなくなるためである。

デジタル署名には時刻情報を含めることが可能であるが、それは通常、デジタル署名を生成するパソコンのシステム時計の時刻が用いられる。この時刻はパソコンの管理者が自由に変更できるため、一般に信頼できる時刻とは考えられない。そのため、署名の再検証を行う際に、署名が有効期間内に作成された本物なのか、その後作成された偽者なのかの区別がつかない。失効が生じた場合にも、同様に失効前の署名なのか失効後の署名なのかを区別することができない。さらに、有効期間後は失効情報さえ発行されないため、失効の有無をも確認できなくなる。

したがって、通常は1~3年程度でデジタル署名の有効性は失われてしまうため、診療録では5年、税務関連文書では7年、その他30年から永年にわたって保存義務のある文書を、真実性を保ったまま保存することができないことになる。

署名有効性延長とは、公開鍵証明書の有効期間や失効、さらにはデジタル署名で利用している暗号技術の脆弱化を克服し、長期にわたってデジタル署名の有効性を維持する技術である。署名有効性延長の要件^①を次に示す(図2)。

要件① デジタル署名の存在時刻を確定する

デジタル署名に信頼のできる時刻を与え、有効期限や失効との前後関係を確認可能とする。

要件② デジタル署名の検証に必要な証拠情報(検証情

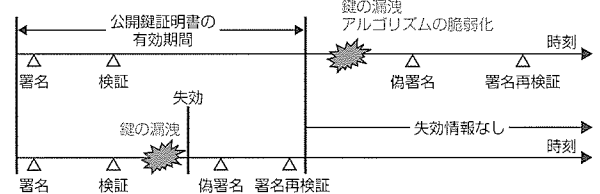


図1. デジタル署名の限界

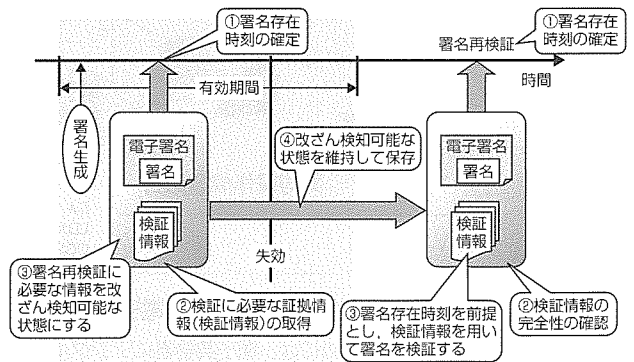


図2. 署名有効性延長の要件

報)を取得する

署名者の公開鍵証明書からルート認証局までの公開鍵証明書のセット、それらの公開鍵証明書に対するCRL (Certificate Revocation List)やOCSP(Online Certificate Status Protocol)⁽²⁾レスポンス等の失効情報を収集する。

要件③ デジタル署名の再検証に必要な情報を改ざん検知可能な状態にする

元々の署名付き電子文書や検証情報を改ざん検知可能な状態とする。

要件④ ③の改ざん検知可能な状態を維持して保存する

③の状態を必要な保存期間にわたって維持する。

要件①から④を満足すれば、次の確認①～③を行うことにより、元々の署名の真偽を区別することが可能となる。

確認① 署名存在時刻を確認する。

確認② 署名付き電子文書や検証情報が改ざんされていないことを確認する。

確認③ 署名存在時刻を想定した検証を、検証情報を利用して実施する。

3. 長期署名フォーマット

前章の要件を満たす方法として、長期署名フォーマット(図3)を利用する方法がある。長期署名フォーマットはRFC3126⁽³⁾等として世界的な標準となっている。この方法では、各要件に次のように対応する。

要件① 署名値に対して標準のタイムスタンプを付与する(ES-Tの署名タイムスタンプ)

要件② 公開鍵証明書のセットとCRLやOCSPレスポンス等の失効情報を格納する(ES-C, ES-Xの検証情報リファレンスと検証情報)

要件③ 署名付き文書(ES), 署名タイムスタンプ, 検証情報リファレンス, 検証情報全体にタイムスタンプを付与する(ES-Aのアーカイブタイムスタンプ)

要件④ 長期にわたって非改ざん性を維持するために、更に全体に対してタイムスタンプを重ねる(外側のアーカイブタイムスタンプ)

タイムスタンプによって要件③④を達成する長期署名フォーマットを利用する方法は、システムや運用の安全性を

仮定することによって同様の効果を得ようとする方法(電子原本管理システム等)と比較して、次のような優れた特長を持っている。

(1) 標準的なPKI技術を用いることでだれでも有効性を検証できる。

(2) 長期署名の構築や延長処理をだれでも実施でき、さらに、途中から他者に処理を引き継ぐこともできる。

(3) 信頼の対象を標準のPKIにおける信頼点に置けばよく、現状では一般的に確認が困難なシステムや運用の安全性に置く必要がない。

(4) タイムスタンプは常にその時点で安全性が確認されている暗号技術を用いてサービスされるため、技術の陳腐化を気にする必要はない。

4. 署名有効性延長システムMistyGuard“EVERSIGN”

長期署名フォーマットを構築するためには、署名タイムスタンプの取得、失効情報を含む検証情報の取得、アーカイブタイムスタンプの取得をそれぞれ適切なタイミングで実施し、長期署名フォーマット内に適切に格納する必要がある。タイミングの管理は極めて複雑であり、一般にその作業を個々の利用者に任せることは難しい。

また、構築された長期署名を検証する際も、元々の署名、署名タイムスタンプ、検証情報、アーカイブタイムスタンプ等をそれぞれ定められた時刻(各タイムスタンプが示す時刻等)を想定した上で実施し、さらに、タイムスタンプの示す時刻と有効期間や失効時刻との整合性を確認した上で真偽の判定をしなければならない。

三菱署名有効性延長システムMistyGuard“EVERSIGN”は、サーバタイプのシステムであり、決められたプロトコルに従って署名付き文書を登録するだけで、長期署名フォーマットを自動的に構築する。EVERSIGNサーバが内部にスケジューラを持ち、各種タイミングやタイムスタンプサービス等の各種データ取得先に関する設定に基づき、処理を自動実行することによってこのような動作が実現される。構築された長期署名データは、やはり決められたプロトコルに従って利用者が取得することができる。

また、長期署名の検証についても、検証プロトコルを用いてEVERSIGNサーバにリクエストを発行することにより、検証結果のレポートを得ることができる。

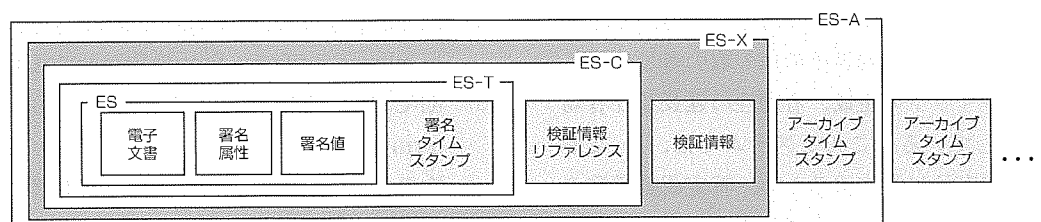


図3. 長期署名フォーマット

EVERSIGNサーバとのリクエスト／レスポンスのやり取りは、EVERSIGNクライアントライブラリを用いることにより、様々なアプリケーションに組み込むことができる。通常、EVERSIGNを単独で用いるのではなく、各種文書管理システムや記録管理システムと連携させることにより長期保存機能を拡張するような形態をとる。

5. 長期署名フォーマット相互運用性実験

2005年10月から12月にかけて、ECOMで長期署名フォーマット相互運用性実験を実施した⁽⁴⁾。この実験は、ECOMで策定した“長期署名プロファイル”への準拠性と各社製品間の相互運用性を確認することを目的としたものである。同プロファイルは、標準の長期署名フォーマットが持つ冗長性とあいまい性を極力排除するために策定したものである。このプロファイルに従った実装を行うことで、長期保存を目的とした長期署名の構築や検証が可能となる。

実験には合計13社の製品又は試作品が持ち込まれたが、当社関連では、三菱電機^(株)情報技術総合研究所の試作品と三菱電機インフォメーションシステムズ^(株)の製品、EVERSIGNが参加した。

実験は、次の二通り実施した。

(1) オフライン検証実験

あらかじめ用意したESフォーマットのデータ(ES-T, ES-X Long, ES-A)、検証情報、設定情報のセットをテスト対象として、各社の実装でオフラインにより有効性を検証する。

(2) オンラインマトリックス生成・検証実験

各社の実装により生成された長期署名テストデータを、他社の実装がエラーなく読み込み、正しく検証できるかどうかを確認する。

当社関連の2つの実装を含み、各社の実装がテストに合格し、ECOMで定めた長期署名プロファイルに準拠することが確認された。

6. 適用事例

EVERSIGNは、2006年5月から某社会インフラ系企業等の電子文書管理システムに組み込まれた形で稼働中である。このシステムは、システム導入企業とその企業との取引企業間で電子契約を行うためワークフローと電子文書・電子化文書の保存管理機能を提供するサービスであり、EVERSIGNは、システム中核の文書保管サーバから、取引会社間で電子署名された契約書その他の取引書類に対して、長期署名フォーマットの生成、有効性の延長及び有効性検証機能を提供している。このシステムでは、e-文書法の改正電子帳簿保存法に対応するため、特定認証業務の認定を受けた証明書と、日本データ通信協会から認定された^(株)PFUのタイムスタンプサービスを利用している(要旨

イメージ図のシステム構成参照)。2006年6月現在の実績では、運用開始直後であることと、初期の利用企業数を限定したこともあって、登録文書ベースで3,000件/月程度の利用にとどまっているが、今後利用企業を増やしていく予定であり、利用規模が大きく拡大する見込みである。

また、今年秋には、某金融機関が提供する全国的な規模の電子契約文書保管サービスでの利用も予定されている。このシステムでは、利用企業数、取扱文書数ともに現在稼働中のシステムを上回る見込みである。このシステムの基本的な構成は、この章で述べた稼働中のシステムとほぼ同じであるが、複数の企業間で利用可能なASP(Application Service Provider)サービスとして提供される予定である。また、公開鍵証明書検証の仕組みとして、OCSPによる失効検証方式が使用される予定である。

7. むすび

標準の長期署名フォーマットに基づき、電子的な文書や記録の真実性及び適正性を長期間にわたって維持できる技術について述べた。ここで述べた方法は、ある特定のシステムに縛られることなく、いつでも、だれでも、有効性の確認や、延長処理の引継ぎができるという利点を持っている。このようなポータビリティは、特に“長期”を考える上では、極めて重要な意味を持つ。ある特定のシステムやサービスに依存するという事は、そのシステムやサービスを提供するある特定の企業や組織に依存するという事であり、ここで言うポータビリティを具備することにより、その企業又は組織の事業継続性に左右されてしまうことがなくなるからである。

ただし、このポータビリティという特長が生かされる前提として、相互運用性が実際に確保されていることが不可欠であるが、ECOMの相互運用性実験により、当社の実装がこの前提を満たしていることが確認されている。

今後予定されている日本版SOX法の施行により、文書や記録の真実性及び適正性の確保とその保存が、今後ますます重視されることになる中、当社の技術や製品がそれらに大いに貢献していくことを期待する。

参考文献

- (1) 宮崎一哉, ほか: 電子文書保存の仕組みと実務, 中央経済社 (2005)
- (2) RFC2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol-OCSP (1999)
- (3) RFC3126: Electronic Signature Formats for long term electronic signatures (2001)
- (4) 次世代電子商取引推進協議会: 長期署名フォーマット相互運用性実験報告書 (2006)

ユーザー情報の多様な変化に対応した アイデンティティライフサイクル管理技術

近藤誠一*
鶴川達也*

Identity Lifecycle Management Technology

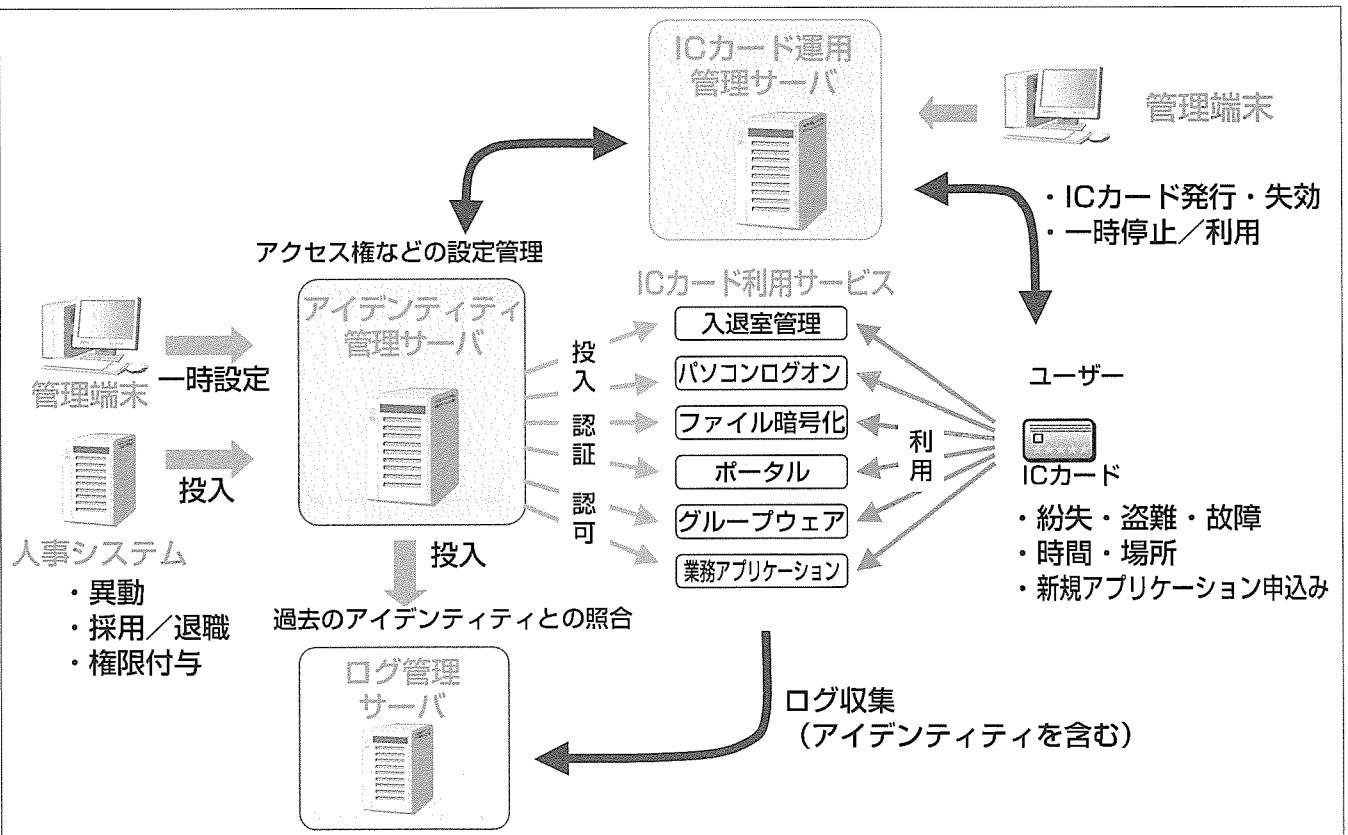
Seiichi Kondo, Tatsuya Tsurukawa

要旨

近年、企業活動のITへの依存度が増大しており、企業の機密情報や個人情報の外部への漏洩(ろうえい)や不正アクセスなどの事件・事故が経営に直結するリスクとして認識されている。情報漏洩に対するセキュリティ対策として、機器・建造物に対する“物理セキュリティ”，計算機上の情報の漏洩・改ざん、偽造の脅威に対する“情報セキュリティ”など様々な方策が導入されている。従来、これらの対策システムを個別に導入してきたが、様々な脅威に対してワンストップで対応していくためには、体系的な導入が有効であると考えられている。特に、“だれが”(人)，“何を”(物、コンテンツ)，“実施できる/した”(アクセス権、実行ログ)といった人とその属性情報をキーとしたアイデンティティを統合管理し、運用の効率化、確実なセキュリティ対策、監査・分析を実現するシステム構成が採用されつつ

ある。

このような情報セキュリティガバナンスを目指した統合型のシステムでは、導入後の人事異動等のユーザーの変化、及びユーザーを識別するために導入されるICカード等の認証デバイスの変化に対して確実に、かつ、速やかに追従することが課題となる。この技術は、入退室管理システム、パソコンログオンシステム、ICカード発行システム、ログ監査システム等のセキュリティ製品、及び業務システムにアイデンティティを提供するアイデンティティ管理システムにおいて、企業活動における人の変化を迅速に反映し、企業活動の継続、セキュリティレベルの維持・向上を実現する。また、長期間蓄積された実行ログに対してアイデンティティの変更履歴データを提供することにより、過去の行為のトレースを可能とする。



変化に対応したアイデンティティ管理システムの構成例

アイデンティティライフサイクル管理技術により、企業情報システムを構成する様々なセキュリティコンポーネント、業務システムが利用するアイデンティティ統合システムにおいて、アイデンティティの変化に対する運用コスト軽減、セキュリティレベルの維持・向上を実現する。

1. ま え が き

近年、企業の機密情報や個人情報外部へ流出する事件が多発しており、社会問題となっている。その対策として、紙文書・媒体・機器・建造物に対する“物理セキュリティ”、計算機上の情報の漏洩・改ざん・偽造の脅威に対する“情報セキュリティ”がとられる。従来これらのセキュリティ対策システムを個別に導入してきたが、様々な脅威に対して継続的に維持・向上させていくためには、体系的な導入が有効であると考えられる。そのため、ユーザーをキーとして、機器、コンテンツに対する行為の実行前のアクセス制御、実行後の監査を行うための基盤であるアイデンティティ管理システムが導入されはじめています。

本稿では、アイデンティティ管理システムにおけるアイデンティティのライフサイクル管理技術として企業向けアイデンティティ管理、ICカード運用管理、デジタルトレーサビリティについて述べる。

2. アイデンティティ管理とその課題

2.1 アイデンティティ管理システム

アイデンティティ管理システムは、ユーザー情報、及びユーザーに割り当てられるアクセス権の管理を行う。図1に示すように、アイデンティティをデータベースで統合管理し、“安心”で“快適”なユーザー認証・認可を実現する。アイデンティティは、入退室管理システム、業務アプリケーションなどに配布される。また、パソコンログオンシステム、持ち出し制御システム、ファイル暗号化システム、Web業務アプリケーションシングルサインオンシステムなどのユーザー認証、アクセス権に従った認可に利用される。

2.2 企業活動における課題

アイデンティティ管理は、導入後の企業活動による以下の変化に追従したライフサイクル管理が課題となる。

(1) ユーザー情報とアクセスポリシーの変化

会社に所属する社員は、入社、退職、異動、昇進、組織変更といったアクセス制御の基になるユーザー情報の属性が変化する。また、セキュリティ対象である機器、コンテ

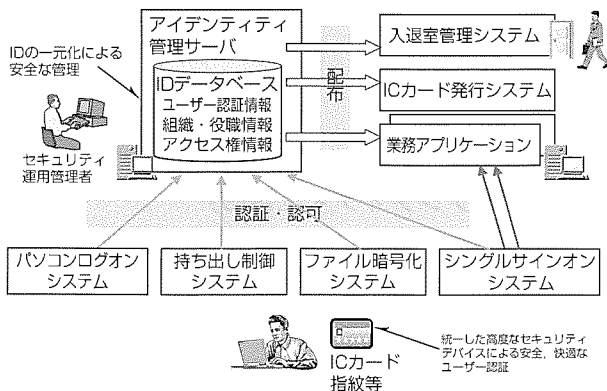


図1. アイデンティティ管理システムの構成

ンツの追加削除、内的／外的要因によるポリシーの改善が行われる。

(2) ユーザーを識別するための認証デバイスの変化

社員、来訪者等の人を識別し、様々なアプリケーションで共用するICカードの導入が進みつつある。しかし、紛失、汚損・破損・故障・盗難等のリスクがあり、企業活動の安全な継続のためには、変化に迅速かつセキュリティポリシーに沿った対応をする必要がある。

(3) 長期保存されたログにおけるユーザーの変化

セキュリティ規格ISO/IEC 27001:2005⁽¹⁾では、監査ログ取得として、“利用者の活動、例外処理、及び情報セキュリティ事象を記録した監査ログを取得すること、また、将来の調査及びアクセス制御の監視を補うために、合意された期間、保持すること”と定めている。一般に、保持期間は長期にわたるため、その間に変化するユーザー情報、機器、コンテンツとの対応が課題となる。

本稿では、各課題に対する解決策を、3章～5章で示す。

3. 企業向けアイデンティティ管理

ユーザーと機器、コンテンツ等のセキュリティ対象を分離してアクセス制御を行う手法としてロールベースアクセス制御RBAC(Role-Based Access Control)モデル⁽²⁾が一般的である。RBACでは、ユーザーとセキュリティ対象への操作の許可をロールを介して間接的に紐(ひも)付けることにより、ユーザーの変化やセキュリティ対象の変化を局所化する効果がある。階層RBACは、更にロールを階層化したものである。2.2節⁽¹⁾で述べたように、一般の企業では、組織、役職といった人事情報を基にロールを定めることが多いため、人事上の変更がロールとユーザー間の設定に大きな影響を及ぼすという課題があった。

そこで、図2(b)に示すように、人事情報に対応するユー

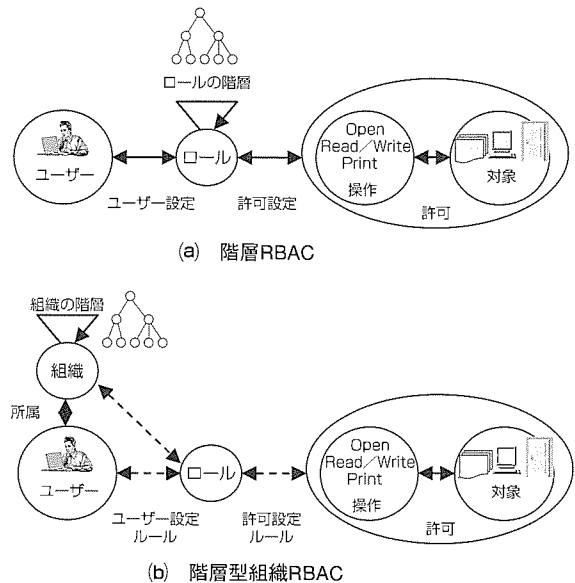


図2. ロールベースアクセス制御RBAC

ザー、組織をロールから独立させた構造を提唱する⁽³⁾。また、ロール-組織間、ロール-ユーザー間の関係を、直接紐付けしないで、論理式で定義したルールによって間接的に指定する。その結果、人事情報の変更時のロールへの影響度を抑えることが可能になる。図3に示すように、PDCAサイクルの各段階において、以下に示す処理を行う。

- PLAN：セキュリティ運用管理者は、セキュリティ対象のアクセスが許可されるユーザーの集合としてロールを定義し、その設定を行う。
- Do：人事異動等のユーザーのライフサイクルに従って、ユーザー情報、組織情報を変更する。
- Check：アイデンティティ管理システムは、過去のログに含まれるユーザーIDを補足するため、PLAN、DOにおける変更履歴を含めたID情報を提供する。

4. ICカード運用管理

ICカードは、企業における社員証として、入退室、パソコンログオン、承認、印刷制御等の利用が広がっている。一方で、2.2節(2)の課題で述べたように、サービスを継続的に利用するためには、図4に示すような、人事異動、出張といったICカードを保有するユーザーの状態の変化、紛失、汚損・破損・故障、盗難、有効期限切れといったICカードの状態の変化に伴い、アクセス権の変更、代替カードへの切り換え、監査ログ出力を迅速にかつ確実にを行う必要がある。特に、代替カードへの切り換えでは、正式なカードとの状態の組合せの整合性維持が課題となる。

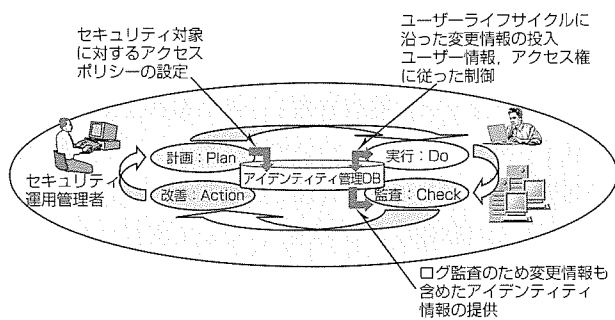


図3. PDCAサイクルの各段階におけるアイデンティティの利用

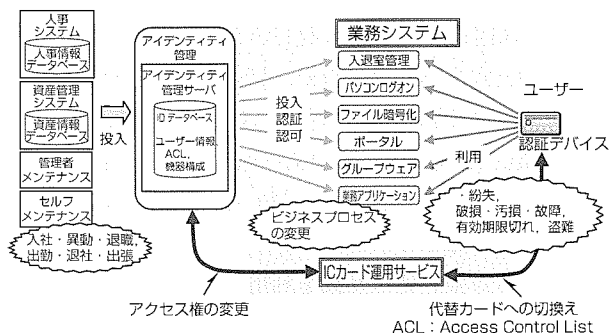


図4. ICカード運用管理システムの構成例

そこで、図5に示すように、ICカードの運用ルールを状態遷移図で定義し、プログラムレスで運用システムを構築する方式を提唱する。運用ルールは以下の手順で定義し、実行する。

- ① 社員用カード、非社員常駐者用カード、訪問者用カード、及び事故に即時対応するための予備カードなどの状態の変化を図に示す遷移図としてプログラムから独立して動的に定義する。
- ② 状態の変化に伴うアクセス権の変更や、対になる予備カードと同時に利用できないといった制約を動作として定義する。
- ③ ①②で定義された運用ルールに従って、状態変化に伴う動作を自動実行する。

このように運用ルールをプログラムから独立した構成を採用したことにより、以下に示す効果がある。

- セキュリティレベル向上
複数のカード間の状態の整合性、アクセス権管理との連動を自動化することにより、故意/過失による人為的な誤った行為を抑制する。
- 運用ルールの異なる環境への対応
要求されるICカード運用ルールが異なる部門に対して、プログラムレスで対応可能である。

5. デジタルトレーサビリティ

2.2節(3)の課題で述べた長期保存されたログにおけるユーザーの変化に対応したデジタルトレーサビリティについて述べる。今日、情報漏洩問題発生時の原因解析などを目的に、様々なアプリケーションやシステムが出力するログの収集保存が行われている。しかし、ログに記録されているユーザーIDの収集元ごとの不一致が複数ログの統合解析を妨げる一因となっている。このような背景の下、アイデンティティ管理の特長の一つである入社・異動・退職といった長期的な変化に対応したライフサイクル管理と連携することでログの解析性を向上させるデジタルトレーサビ

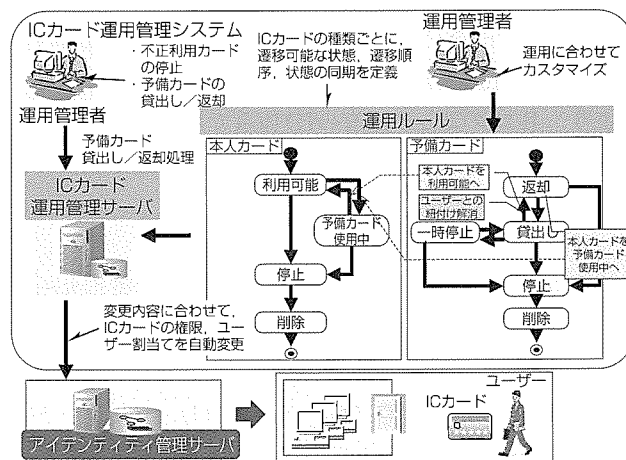


図5. 運用ルールを利用した実装例

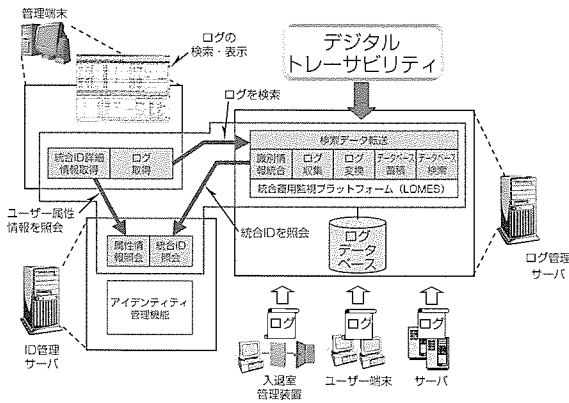


図 6. デジタルトレサビリティを用いたシステム構成例

リティについて述べる。

5.1 収集保存したログの活用とその課題

ログに記録されるユーザーIDに着目すると、収集保存したログを利活用する上で、以下に挙げる課題がある。

- 複数ログの統合解析が困難
ユーザーIDが各ログ固有のIDで記録されており、異なるログ同士を結び付けた統合解析が難しい。
- ユーザーの属性情報を解析に利用できない
ログには、通常、ユーザーIDに付随する属性情報(氏名、所属名など)は記録されず、解析に利用できない。

5.2 アイデンティティ管理との連携による解決

デジタルトレサビリティを利用したシステムの構成例を図6に示す。端末やサーバ、物理セキュリティ装置などからログを収集し、ログ管理サーバ上に蓄積保存する。さらに、アイデンティティ管理機能を提供するID管理サーバ、ログ管理サーバに蓄積保存したログを検索・表示する管理端末から構成されている。

(1) 統合IDの照会とログへの反映

ログ管理サーバでは、ログを収集した後、ログに記録されているログ固有のユーザーIDに対応する統合IDをID管理サーバに照会し、それをログに反映してから蓄積する。

ここで、ログ固有のユーザーIDは、ログオンアカウントやメールアドレスなどを指し、統合IDは、社員番号のようにユーザーを一意に特定することができるIDを指す。

統合IDの照会と反映をすべてのログに対して施すことにより、各ログごとに固有のID体系で記録されたユーザーIDを紐付けることができ、異なるログ同士を統合したログ解析が可能となる。

(2) 属性情報を利用した解析

管理端末でログを検索・表示した後に、ID管理サーバと連携し、統合IDに付随する一部の属性情報を照会し追加表示することが可能である(図7)。これら属性情報をログ蓄積時に反映するとログサイズが増大し、ログデータベースの容量が無駄に使われてしまうが、検索して絞り込んだ後にログに反映することで、この問題を解決しつつ、ロ

利用者ID	出力ファイル	内容
0010022	CustomerList2005.pdf	監査(ファイルの更新)
0020013	CustomerList2005.pdf	監査(外部メディアへ)
0010007	CustomerList2005.pdf	監査(ファイルの印刷)
0010017	Cust	利用者ID
0020011	Cust	氏名
0010018	Cust	所属
0010016	Cust	出力ファイル
0010007	Cust	0010022 高岡三郎 国内営業部 CustomerList2005.pdf 監査(フ
0010014	Cust	0020013 佐藤竹子 国際営業部 CustomerList2005.pdf 監査(例
	Cust	0010007 大谷七郎 国内営業部 CustomerList2005.pdf 監査(フ
	Cust	0010017 橋山祐子 国内営業部 CustomerList2005.pdf 監査(フ
	Cust	0020011 中村花子 国際営業部 CustomerList2005.pdf 監査(フ
	Cust	0010018 相田百合子 国内営業部 CustomerList2005.pdf 監査(例
	Cust	0010028 内村九郎 国内営業部 CustomerList2005.pdf 監査(例
	Cust	0010014 里中竹子 国内営業部 CustomerList2005.pdf 監査(フ

図 7. 属性情報の統合表示

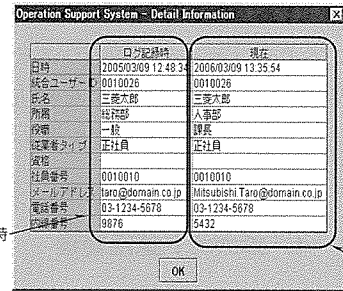


図 8. 過去と現在の人事情報表示

グ解析時の効率的な属性情報の利用が可能となる。

また、同じくID管理サーバと連携し、統合IDから対応する人事情報を引き出して表示することで、逐次実体情報を参照しながらログを解析することが可能となる(図8)。解析対象のログが古く該当ユーザーが退職しているような場合でも、ログレコードの日付時刻から在籍当時の人事情報を引き出して表示することにより、過去にさかのぼったログの解析性の確保が可能である。

6. むすび

情報セキュリティガバナンスを実現するために必要となるアイデンティティの統合管理と、その多様な変化に対応したライフサイクル管理について述べた。アイデンティティの運用管理に対して、利便性を実現した“快適”、システムを利用した自動化による“安全”、そして実行ログの監査へのアイデンティティ履歴の提供による“発展”を更に追求していきたいと考えている。

参考文献

- (1) 財団法人規格協会：国際規格ISO/IEC 27001：2005, 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, ISO/IEC (2005)
- (2) Sandhu, R.S., et al.: Role-Based Access Control Models, IEEE Computer, 29, No.2, 38~47 (1996)
- (3) 近藤誠一, ほか：ルールベースアクセス制御情報の多バージョン並行処理制御を利用した監査ログトラッキング手法, 情報処理学会論文誌, TOD 28 (2005)

ユビキタスセキュリティ —監視映像情報セキュリティ—

山口晃由*
山田敬喜**
松井 充***

Ubiquitous Security—Information Security for Surveillance Camera System—

Teruyoshi Yamaguchi, Keiki Yamada, Mitsuru Matsui

要 旨

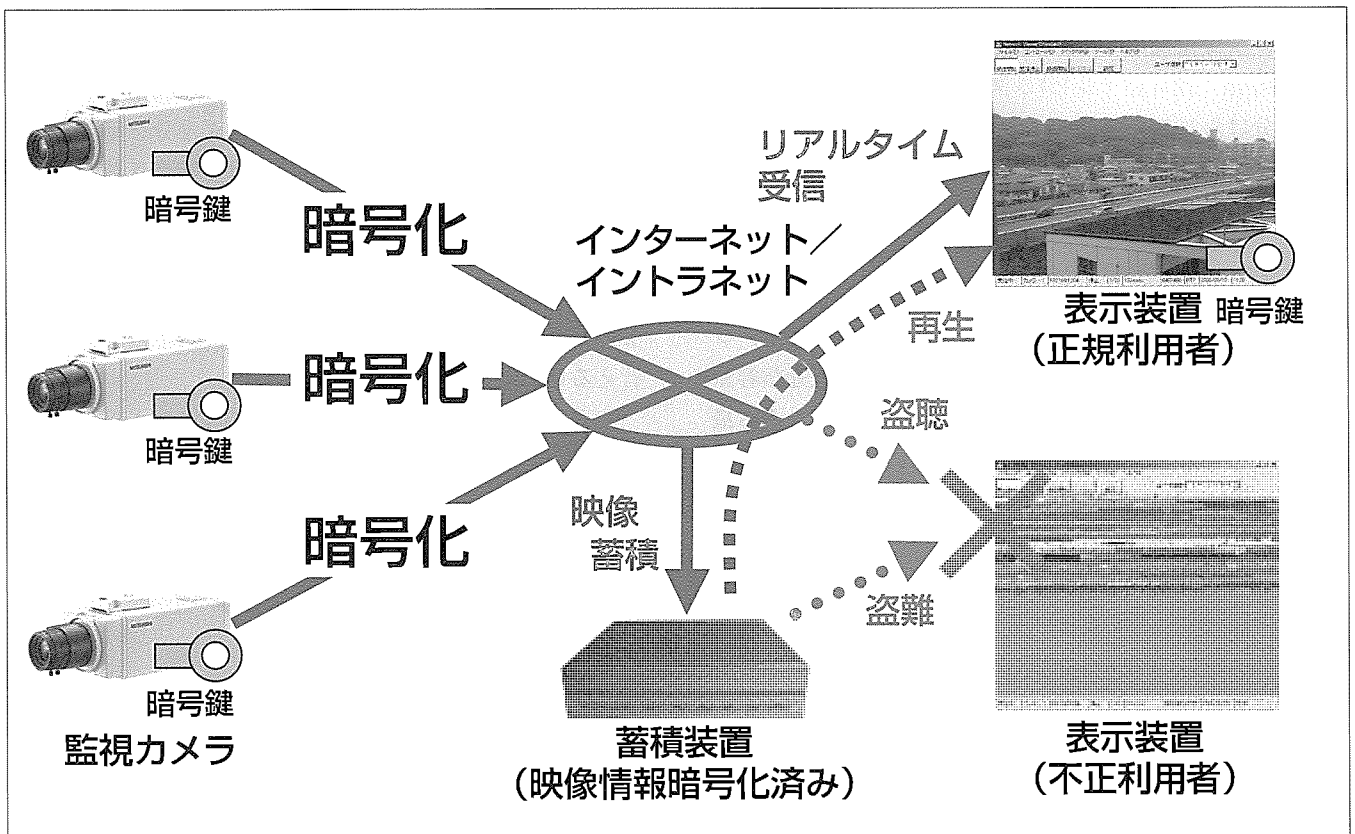
近年の犯罪率増加と犯罪検挙率減少を背景として、ビル・マンション・商店街等を中心に、監視カメラを用いた映像監視システムを導入する動きが広がっている。一方で、無制限な監視カメラの設置はプライバシーを侵害するという声も少なからずある。映像情報を適切に扱うことで、映像監視への理解を得ることができる。特に通信路の盗聴や映像を蓄積したストレージの盗難といった不正な漏洩(ろうえい)から、映像情報を保護する必要がある。

このような漏洩から映像情報を保護する方法として、映像を暗号化し、閲覧可能者を限定する方法がある。しかしながら、映像監視システムでは、CPU(Central Process-

ing Unit)速度やメモリ容量などのハードウェア的な制約、画像サイズ・フレームレート(1秒間に何枚の映像を流せるか)などの性能的な制約の下で、映像を暗号化することが要求される。特に、監視カメラや表示装置では、演算に組み込みマイコンを用いるため、暗号処理は非常に重い処理となる点が問題である。この解決のために暗号処理ハードウェアを追加することは、大幅なコスト増につながり、好ましくない。

本稿では、映像監視システムにおいても要求される性能を満たしつつ暗号処理を実現する技術について述べる。具体的には、組み込みマイコンでも高速に処理が行える暗号アルゴリズム、及び高効率画像暗号化法について論じる。

特集
I



映像監視システムにおける映像情報の暗号化

映像監視システムは、多数の監視カメラで撮影した映像を蓄積し、必要に応じて表示を行う。近年、映像監視システムもデジタル化が進み、インターネットや共用LAN(Local Area Network)を使って映像を配信している。そこで、通信・蓄積の過程での映像の盗聴や盗難に対して映像情報を保護するために、カメラで撮影した映像をリアルタイムで暗号化し、表示装置においてリアルタイムに復号する。監視カメラと同じ暗号鍵(かぎ)を持つ正規利用者は映像を正しく表示できるが、暗号鍵を持たない不正利用者は映像を正しく表示できない。

1. ま え が き

映像監視システムは、監視カメラによって監視及び映像の蓄積を行い、犯罪行為の抑止や証拠収集を行うシステムである。近年の犯罪件数増加や犯罪検挙率低下などの社会背景を受け、防犯を目的として映像監視システムを導入する施設が増加している。その市場規模は930億円とも言われ、今後ますます増加する傾向にある。最近では、市街や駅舎にも設置するケースも見られる。

一方で、無制限な監視カメラの設置がプライバシーを侵害するおそれもある。映像監視システムの設置に際しては、監視映像の安全かつ適切な管理が求められる。2005年に施行された個人情報保護法では、監視映像も個人情報とみなされ、運用によっては管理に法的責任が生じる可能性もある。特に、通信路の盗聴や映像を蓄積した記録装置の盗難といった不正漏洩から映像情報を保護することが必要である。

本稿では、不正な漏洩に対する映像情報の保護という課題に対し、映像情報を暗号によって保護する技術について述べる。

2. 映像監視システム

2.1 CCTVシステム

現在、映像監視システムは大きくCCTV(Closed Circuit Television：閉回路テレビ)システムとWebカメラシステムとに分けられる。前者は、カメラと蓄積装置・表示装置を専用線で結び、カメラからの映像を常時蓄積・表示するものである。高画質、高フレームレートを特長とする。後者は、カメラとパソコンをインターネットなどで結び、カメラがWebサーバ機能を持っており、パソコン(ブラウザ)からアクセスがあったときだけ映像を送信する。画質、フレームレートはCCTVシステムに劣るものの、低通信容量、低価格、導入の容易さなどを特長とする。しかしながら最近では、後述するデジタルCCTVシステムの登場で、CCTVとWebカメラとの境界は曖昧(あいまい)になりつつある(図1)。

2.2 デジタルCCTVシステム

従来、CCTVシステムはアナログが主流であったが、近年、IP(Internet Protocol)網を使ったデジタルCCTVシステムが普及しつつある。同軸ケーブルを用いて信号を送るアナログCCTVシステムとは異なり、デジタルCCTVシステムでは、映像を圧縮し、LANを使って送信する。既設IP網を利用できるため、設置コストの低減や容易な増設が可能となる。本稿で述べる映像の暗号化は、デジタルCCTVシステムを対象とする。

多くのデジタルCCTVシステムやWebカメラシステムでは、映像データにモーションJPEG(Joint Photographic

Experts Group)やMPEG(Motion Picture Experts Group)などの圧縮を施して送信する。モーションJPEGは高画質であるがデータサイズが大きくなる傾向にあり、MPEGはその逆となる。映像データのフォーマットはベンダーによりまちまちであるが、三菱電機デジタルCCTVシステム“DIGITALMELOOK”はモーションJPEGを採用している。一方、DIGITALMELOOKを始め、多くのデジタルCCTVシステムでは、VGA(Video Graphics Array)(640×480)の画像を30fps(frame/sec)で送信する。そのため、暗号処理もこの性能を落とすことなく実現する必要がある。

3. デジタルCCTVシステムにおける監視映像の暗号化技術

不正な漏洩から映像を保護するため、カメラから出力する前に映像を暗号化し、表示装置で復号して表示する。このことで、通信路の盗聴に対して映像を保護することができる。また、映像を暗号化したまま蓄積することで、蓄積装置の盗難に対しても映像を保護できる。

デジタルCCTVシステムに暗号を組み込む場合、カメラや表示装置が大量の映像を高速に暗号化/復号しなければならない。しかしながら、これらの機器は組み込みマイコンを用いており、決してリソースが豊富でない。そのため、組み込み機器においても、高速に画像を暗号化/復号する技術が必要となる。

JPEGやMPEGなどで圧縮された画像を高速に暗号化する方法として、JPEGやMPEGのヘッダ部分を暗号化する手法がある。これらのヘッダ部分には圧縮されたデータを復元するために必要な量子化テーブルやハフマンテーブルなどの情報があり、ここを暗号化することで、画像データの復元を防止できる。画像サイズに依らず、ヘッダ部分はせいぜい600~700バイト程度であるので暗号処理も高速に行える(図2)。

しかし、組み込み機器でJPEGやMPEGのエンコードを行う場合、量子化テーブルやハフマンテーブルなどのパラ

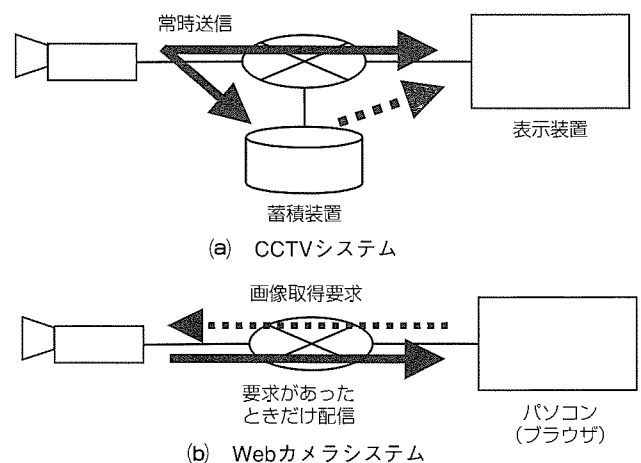


図1. CCTVシステムとWebカメラシステムの違い

特集
I

メータに固定値を用いることが多い。そのため、一度正しく復号できたヘッダ情報入手できれば、それを暗号化されたヘッダと置き換えることで、映像を復元されるおそれがある(図3)。したがって、暗号化はエンコードされたイメージ本体に対して行う必要がある。

エンコードされたイメージ本体のデータサイズは画像サイズや圧縮レベルに依存し、通常、ヘッダ部分の数十倍から数百倍程度のサイズがある。これを30fpsで処理するには、1枚当たり33ms以内に暗号処理を含むすべての処理を行わなければならない。さらに、監視カメラへの実装の場合、画像のエンコードやパケット処理のオーバーヘッドがあるため、暗号処理に割ける時間は更に短くなる。

この問題に対し三菱電機では、組み込み機器用高速暗号アルゴリズムの開発とJPEG画像の高効率暗号化法の開発により高速処理を実現した。

3.1 組み込み機器用高速暗号アルゴリズム“BROUILLARD”(ブレイヤール)の開発

組み込み機器用高速暗号アルゴリズムBROUILLARDは、ソフトウェアでの超高速化を目標として開発された。大き

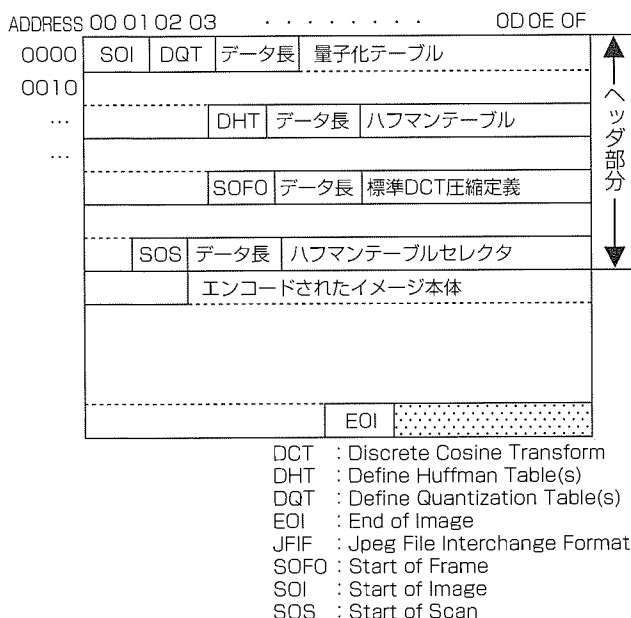


図2. JPEG画像(JFIF)フォーマットの一例

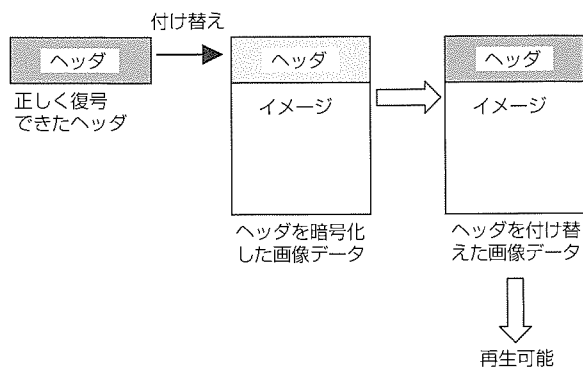


図3. ヘッダの付け替えによる画像再生

なメモリ空間のランダムアクセスによって高速性と安全性を実現している。Pentium 4 (3 GHz)^(注1)で8 Gbpsの暗号化速度を実現することができる。

表1に、SH-4(240MHz)^(注2)マイコン上にTriple-DES(Data Encryption Standard), MISTY1, BROUILLARDを実装し、31kバイト相当のデータ(三菱電機デジタルCCTVシステムが出力するJPEG画像1枚分に相当^(注3))を暗号化したときの処理時間を示す。

表から、Triple-DESでは画像データ1枚の暗号化に128msかかってしまい、30fpsを満たす性能を出せない。MISTY1では30fpsに近い性能を出せるが、実際には暗号処理以外の負荷がかかるため、MISTY1でも実現は難しい。これに対してBROUILLARDでは、暗号処理を高速に行えるため、30fpsを十分に満たす性能を期待できる。

3.2 JPEG画像の高効率暗号化法の開発

BROUILLARDの開発により、30fpsを満たす暗号処理が期待できるようになった。しかしながら、表示装置で複数台のカメラの映像を同時に表示する場合、更なる高速化が要求される。暗号そのものの高速化に加え、暗号処理を行うデータサイズの削減で、処理全体の更なる高速化を行う。映像情報の暗号化の目的は、不正利用者に映像を再生させないことであるため、それを実現できれば必ずしも全イメージデータを暗号化する必要はない。そこで、暗号化するイメージデータの位置を最適化することで少ないデータサイズで画像を不可視にする手法を開発した。

表2に、SH-4(240MHz)によってイメージ本体をすべて暗号化した場合と、暗号化するデータの位置を最適化した場合の処理時間を示す。暗号アルゴリズムはBROUILLARDを用いた。今回開発した方法により、イメージ全体を暗号化する従来の方法に比べ2.5倍の性能向上を図ることができた。

次に、暗号化するデータの位置を最適化した場合の画質を評価した。原画像(図4)に対してイメージ本体をすべて暗号化した画像(図5)と、暗号化するデータの位置を最適化した画像(図6)を示す。

(注1) Pentiumは、Intel Corp.の登録商標である。

(注2) SH(SuperH)は、(株)ルネサステクノロジの登録商標である。

(注3) VGAサイズ、圧縮率1/20の場合

表1. 31kバイト相当のデータを暗号化したときの処理時間

暗号アルゴリズム	処理時間 (ms)
Triple-DES	128
MISTY 1	33.1
BROUILLARD	4.45

表2. JPEG画像の高効率暗号化法による処理時間の比較

画像暗号化法	処理時間 (ms)
イメージ全体を暗号化した場合	4.45
暗号化するデータの位置を最適化した場合	1.74

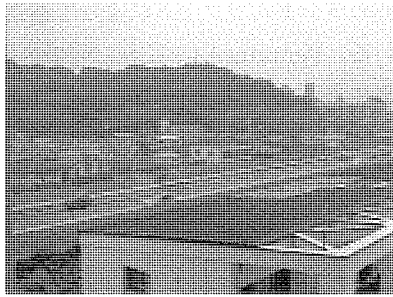


図4. 原画像

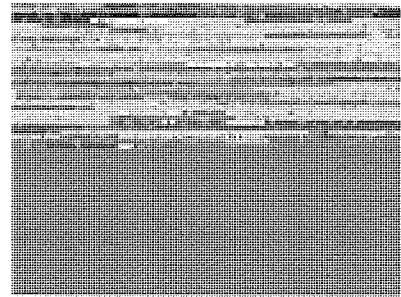


図5. 暗号化画像(イメージ本体すべてを暗号化)

図6下部のブランク部分が図5下部のブランク部分に比べ小さいことが分かる。これは暗号化されたJPEG画像を復号する際に、ハフマン復号によって得られたデータサイズの差によるものと考えられる。ハフマン復号によって得られたデータサイズが画像の表現に求められるデータサイズより小さい場合、足りない分がブランクで表示される。イメージ全体を暗号化した場合に比べ、暗号化するデータの位置を最適化した場合はハフマン復号によって得られたデータサイズが大きいため、ブランクの領域が小さくなったものとする。しかしながら、暗号化するデータの位置を最適化した場合でも、原画像の推定を困難にするには十分な攪拌(かくはん)が行われていることが分かる。

4. むすび

本稿では、デジタルCCTVシステムにおける映像情報の暗号化技術について、暗号処理に求められる要件と、要件を実現するための技術について述べた。

今後は、暗号処理の更なる高速化や、映像の暗号化に用いる暗号鍵の安全な管理法の開発を行う予定である。

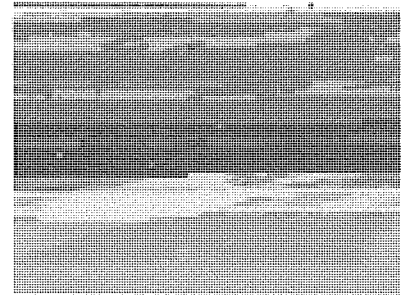


図6. 暗号化画像(暗号化するデータの位置を最適化)

参考文献

- (1) 2004セキュリティ関連市場の将来展望, 富士経済
- (2) JIS X4301 連続階調静止画像のデジタル圧縮及び符号処理-第1部 要件及び指針
- (3) 機器組み込み用高性能暗号アルゴリズム「BRUME」と「BROUILLARD」を開発, 三菱電機広報発表資料, 開発No.0517



// 設計開発プロセスの革新における深層

Depth in Innovation of Design and Development Process

藤田喜久雄
Kikuo Fujita

設計開発プロセスを革新しようとする動きは、時々の要請や背景とも呼応しながら、時として、あるキーワードを核にした盛り上がりを見せる。このところ、直面する課題や利用可能な手段を踏まえてフロントローディングに向けた様々な取り組みが盛んに進められているようであるが、国際的な設計工学の学術動向の中でFront Loadingという言葉を見ることは比較的稀(まれ)である。一方、この15年ほどの我が国での動向を振り返ると、設計開発プロセスについての新しいコンセプトが一過性のキーワードとして消費されてきた傾向も否めない。一連の対比には、その良し悪しはともかくとして、我が国での設計開発プロセスが経験的に発展してきたことが作用しているように思える。改めてそのことを踏まえつつ複雑化していく製造業の将来を見据えれば、目下のフロントローディングについての取り組みを真に実りあるものとするためには、より深層にある普遍的な課題を認識した上で、長期にわたって継続して目指していくべきこと、その下で時々に取り組むべきこと、それらを相互に関連付けた地道な努力も求められている。

設計開発プロセスについての課題は多様であるが、対象であるシステムの複雑化とそれを導き出す際の生産性の向上を2つの座標軸として整理することが有益である場合もある。フロントローディングに絡めれば、前者は複雑化による領域横断性の拡大に対して一連の内容を総合的に取り上げて異なる技術領域からの検討を統合して行えるようにすることに、後者はその実行をより高効率でより短期間で行えるようにすることに対応する。つまり、フロントローディングについての活動として、デジタルエンジニアリング技術や情報技術の導入を進めて処理のスピードや領域間の見通しなどを改善したり、又は、業務形態を改めてプロ

セスの効率化を進めたりすることは妥当な方策であると言える。しかしながら、それらは、15年余りの間、キーワードをすげ替えながら進められてきた様々な取り組みの延長線上にあるものでもある。

製造業での状況はともかくとして、このところ、高等教育のあるべき姿を展望する際に“知識基盤社会(Knowledge-Based Society)”という言葉が象徴的に用いられている。端的に言えば、科学や技術における知識の蓄積が20世紀を通じて相当に進んだことを受けて、21世紀においては、知識の財としての意味が拡大し、その生産における様式すらも問われるようになってきており、高等教育機関にはそれらのことを前提とした進化が求められている。設計や開発は生産を通じて製品に埋め込むべき知識を創出する活動である。そうであれば、高等教育機関に課せられている知識の重要性は設計生産プロセスについての課題に直結するものとなる。この15年余りの間の設計開発プロセスについての動向は、上述のように最近のフロントローディングに関連するものをも含めて、おおむね、あらかじめ想定されている枠組みのもとでの知識生産の合理性や効率性を高めるためのものとして展開されてきた向きがある。それらは今後も是非の事項であり続けるが、長期的には、それらの背後にある事項、例えば、そもそもの設計者や技術者自身の生産性の刷新にも注意が払われるべき時代に差し掛かりつつあるように思える。それについては、例えば、新たなコンセプトの構想力や異なる領域間の連携におけるコミュニケーションを含む人的な問題、前提となる枠組みを時々に応じて柔軟に編成していくことのできる能力など、設計開発プロセスを革新していくための課題は新たな次元へと深まっていくはずである。

フロントローディング型開発設計への取り組み



竹垣盛一*



原島忠雄**

Activities for Realization of Front-Loading Product Design

Morikazu Takegaki, Tadao Harashima

要旨

市場ニーズの多様化・高度化と製品ライフサイクルの短期化が進む中、顧客要求に合ったコスト競争力のある製品のタイムリーな市場投入が求められている。そのためには開発設計プロセスの革新による開発期間の短縮が必要であり、開発初期段階で徹底的に製品品質の作り込みを行うフロントローディング型開発への移行が鍵(かぎ)になる。

本稿では、三菱電機におけるフロントローディング型開発設計実現に向けた取り組みについて述べる。

ソフトウェア開発、ASIC(Application Specific Integrated Circuit)開発では、ますます複雑化する要求機能に対し、仕様設計段階での品質向上の手段としてUML(Unified Modeling Language)活用による仕様の見える化を進めるとともに、ソフトウェア大規模化/ゲート規模増大に対応した再利用性向上、初期検証技術高度化による開発期間短縮に取り組んでいる。

また、高密度実装製品開発では、筐体(きょうたい)の小形化/高集積化と、動作周波数増大/消費電力増大(高発熱化)に対応し、開発初期段階での機構・熱・EMI(Electro Magnetic Interference)解析等のFOA(First Order Analysis)手法の適用と三次元CAD(Computer Aided Design)モデル活用による実装構造検証を展開することで、試作段階で発生する手戻りの削減を図っている。

フロントローディング設計のもう一つの効果として、新製品開発における製品の最適化が挙げられる。候補となる設計案に対し、開発初期段階で解析検証技術を適用し、設計案を絞り込むことで、目標性能/コスト実現に向かう開発工程全体の効率化、設計工数削減、試作費削減が可能となる。

さらに、フロントローディング型開発設計適用によるプロセス改善を継続的に実践し拡大していくには、定量的指標に基づく改善効果の追跡が必要である。そのために、対象製品開発状況(進捗(しんちやく)、課題)の見える化と共有化を実現する開発管理環境の構築に取り組んでいる。

1. まえがき

フロントローディング型開発設計の考え方を図1に示す。フロントローディング型開発設計の目的は、設計自由度の高い開発初期段階で製品仕様の最適化(合理的判断に基づ

く最善の目標設定)を図るとともに、基本/詳細設計、製造/組立て(ソフトウェアの場合はコーディング)、試験と進む工程の中で、前工程から流出した不具合による手戻り発生を未然に防ぐことである。

2. ソフトウェア・ASIC開発におけるフロントローディング

図2に、ソフトウェア開発における欠陥の発生時期と修正コストの関係を示す。縦軸の値は常用対数となっており、欠陥の検出時期が遅くなるほど修正コストがけた違いに大きくなる。ASIC(Application Specific Integrated Circuit)開発の場合も傾向は同様であるが、ASICを製造する工程が入るため、製造後に重大な不具合が検出されASICの作り直しに至ると、数千万円の再製作コストが上乗せされる。修正コストを抑制するためには、要求分析や設計の各段階で入り込んだ欠陥を、入り込んだフェーズで取り除くことが重要である。

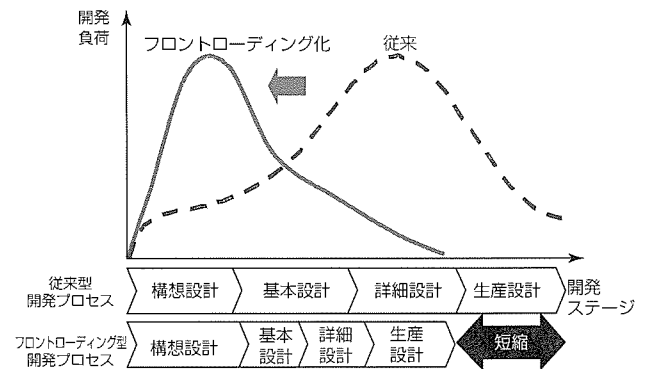


図1. フロントローディング型開発設計

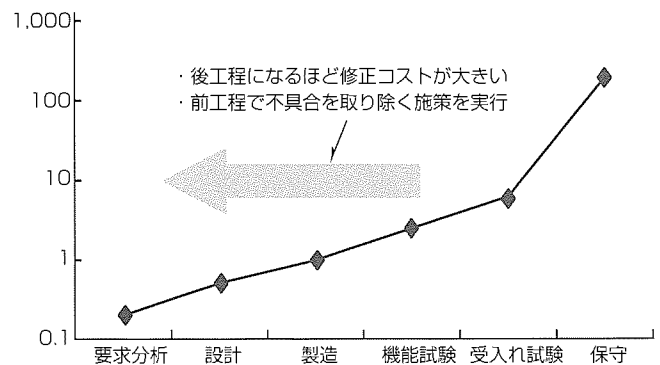


図2. ソフトウェア開発における欠陥発生時期と修正コスト(実装=1の相対値)⁽¹⁾

図3に、ソフトウェア開発における設計フロントローディング化実現のための取り組みを示す。要求分析で、従来の自然言語による要求仕様の記述では、複雑な要求の曖昧(あいまい)さや矛盾を検出し取り除くことが困難である。ソフトウェア開発では、要求仕様を国際標準の記法であるUML(Unified Modeling Language)で図式表現することによって、仕様に見える化、分かる化を実現し、要求仕様を定義する段階でレビュー性を向上しており、ASIC開発でも同様の取り組みを開始している。

設計段階でも、UMLを活用することによって要求仕様と設計の連続性を高め、設計段階での見える化を進めることによってレビュー性を向上させている。

ASICを記述するハードウェア記述言語(Hardware Description Language : HDL)及びソフトウェアのコーディング段階では、可読性/保守性を高め、欠陥を混入しにくくするため、コーディング規約を定めている。さらに、コードを静的に解析する技術を活用して規約遵守状況のチェックを自動化し、コードの品質確保を図っている。

試験段階では、試験設計への品質工学の導入により、試験網羅度の向上と試験組合せ項目数の削減を同時に実現している。また、ASICの試験では、詳細設計段階であるHDLのコーディング後の検証だけではなく、その前の機能設計段階でも言語によるモデル化を行い、早期に機能レベルの検証を実施することで、初期検証を充実し、後工程に流出する不具合を削減している。

さらに、開発プロジェクトの各ホールドポイント単位での進捗(しんちやく)度を把握し、同時に各フェーズにおけるドキュメントや課題リストを共有することによって開発状況の見える化を行い、課題の共有や漏れの防止、進捗にかかわる問題の早期検出に取り組んでいる。

3. 高密度実装製品開発におけるフロントローディング

高密度電子機器の開発では、筐体(きょうたい)の小型/薄型化、電子回路の動作周波数増大、高発熱化トレンドの中で、設計検証技術の向上が求められている。

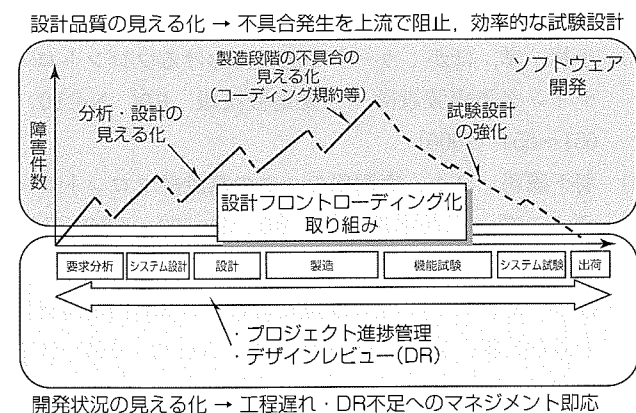


図3. ソフトウェア開発における設計フロントローディング化の取り組み

従来は、構造強度/熱問題への対応を試作後の試験結果に基づき実施したり、信号伝送線路ノイズによる誤動作やEMI(Electro Magnetic Interference)放射ノイズ試験への対応を規格試験段階で実施することが通常であった。しかし、機器の高密度化・高機能化によって対策期間が増大し、同時に、製品ライフサイクルの短期化に伴う開発期間短縮が不可欠の状況となってきた。

そこで、これらの対策技術を設計ルールとして設計段階で極力作り込み、同時にデザインレビュー時にチェックする仕組みを構築して試作後の設計手戻りを削減することで、開発工期の短縮と製品の品質向上を図っている(図4)。

また、変更自由度の高い開発初期段階で設計解を求め、コストと機能仕様の適切なバランスを図ることで、製品コスト削減にも寄与している。

構造強度設計や熱設計では、設計フェーズに応じた詳細度の解析検証を実施し、各フェーズでの設計完成度を上げる取り組みを行っている。

まず、構想設計段階でのFOA(First Order Analysis)手法として、設計知識を凝縮した表計算シートを作成し、例えば高密度実装機器の熱設計で、内部機器発熱量と概略構造に基づく冷却方式選択(自然空冷/強制空冷)等を実施している。

詳細設計段階では三次元設計データを活用し、詳細な解析モデルでの熱流体解析や強度解析等を行い、より精度を上げて各構造パラメータやユニットの配置を決定している。

これらの取り組みにより、試作段階での設計見直しによる大きな設計手戻りを防いでいる。

さらに、三次元データを、設計フェーズにとどまらず、営業、工作、検査等のフェーズで活用することによって、製品ライフサイクル全体での品質向上と業務効率化を図っている(図5)。例えば、エレベーターの営業設計段階での仕様打合せにおけるCG(Computer Graphics)アニメーションの活用、製造準備段階における組立て性の事前検討、

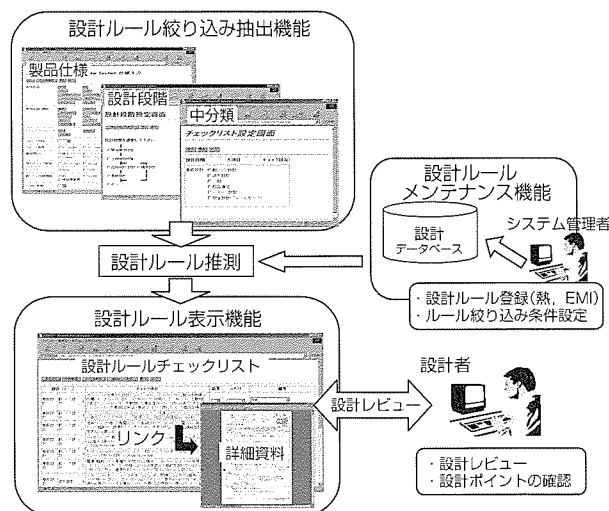


図4. 設計ルールチェックシステム

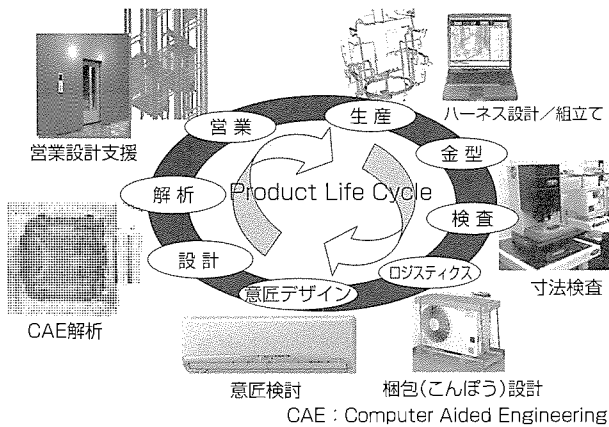


図5. 製品ライフサイクルでの三次元データの活用例

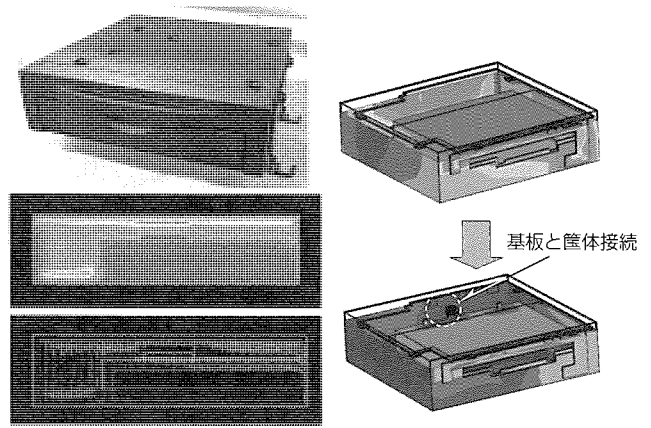


図6. カーナビ開発における熱, EMIシミュレーション

外部に製造委託している部品の受入れ寸法検査における三次元測定装置の導入等が挙げられる。

4. 新製品開発におけるフロントローディング設計事例

2章, 3章でフロントローディング化の取り組みについて述べたが, 具体的に以下のような新製品開発で, 開発初期段階での設計検証技術適用による効果を上げている。

詳細はこの号の特集論文で述べる。

- (1) 社会インフラ分野のソフトウェア開発におけるUML, 静的解析手法, 試験技法の適用⁽²⁾
- (2) カーナビゲーションシステム開発における熱, EMIシミュレーション技術の適用⁽³⁾ (図6)
- (3) 全閉型車両用モータ開発における冷却方式検討のための熱流体シミュレーション技術の適用⁽⁴⁾ (図7)
- (4) 大型映像装置開発における高速伝送路設計への回路シミュレーション技術の適用⁽⁵⁾ (図8)

これらの製品開発では, 性能・機能, 信頼性, コスト等, 既存製品に対してより高い設計目標を, 計画された開発期間内に実現することが必要であった。開発初期段階からシミュレーション技術を駆使することで, 設計案の創出とその妥当性検証を実施し, 目標性能を計画された開発期間で実現している。

5. むすび

以上, 各分野でのフロントローディング型開発設計の必要性と具体的取り組みの概要を述べた。近年の製品開発では, 品質向上はもちろんのこと, コストダウン, 納期短縮の要求が更に増大しつつあり, これにこたえていくためには, 開発設計における手法/プロセスの更なる改善が必要である。今後も, フロントローディング型開発設計への取り組みを継続的に強化していく所存である。

参考文献

- (1) Davis, A. M.: Software Requirements-Objects,

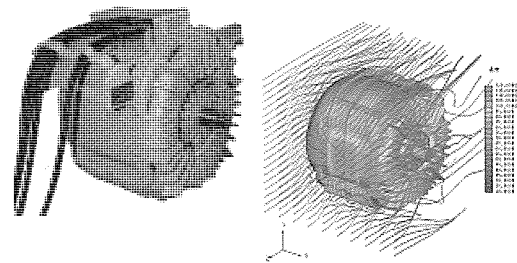


図7. 全閉型車両用モータ開発における熱流体シミュレーション

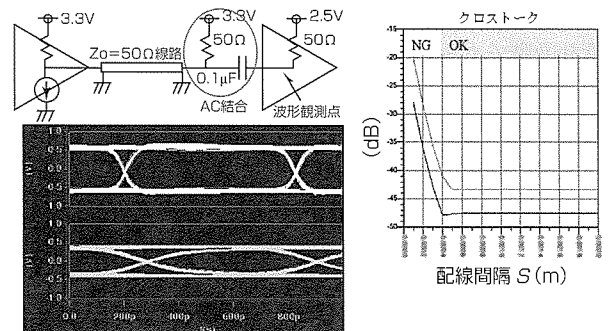


図8. 大型映像装置開発における回路シミュレーション

Functions, & States, Revisions, Prentice Hall, Englewood Cliffs, NJ

- (2) 安江 悟, ほか: 社会インフラシステム開発におけるソフトウェア開発プロセス改善, 三菱電機技報, 80, No.10, 643~646 (2006)
- (3) 小林 孝, ほか: カーナビ開発におけるフロントローディング型実装設計, 三菱電機技報, 80, No.10, 651~654 (2006)
- (4) 羽下誠司, ほか: 車両用モータの熱設計フロントローディング, 三菱電機技報, 80, No.10, 659~662 (2006)
- (5) 島寄 陸, ほか: 大型映像装置におけるGbps高速信号設計技術, 三菱電機技報, 80, No.10, 667~670 (2006)

開発状況の見える化を実現する 開発管理システム

長江雅史* 川北泰之*
今村 剛**
篠崎順子**

Development Management System : Visualization for Status of Development

Masashi Nagae, Tsuyoshi Imamura, Junko Shinozaki, Yasuyuki Kawakita

要 旨

近年、製造業では、世界的規模でのコスト競争の激化とともに、顧客要求に応じた高品質の製品を短期間に開発し市場に提供していくことが求められている。このような状況の中、製品開発の現場では、この要求を満足するため、開発マネジメント力の強化が切望されている。

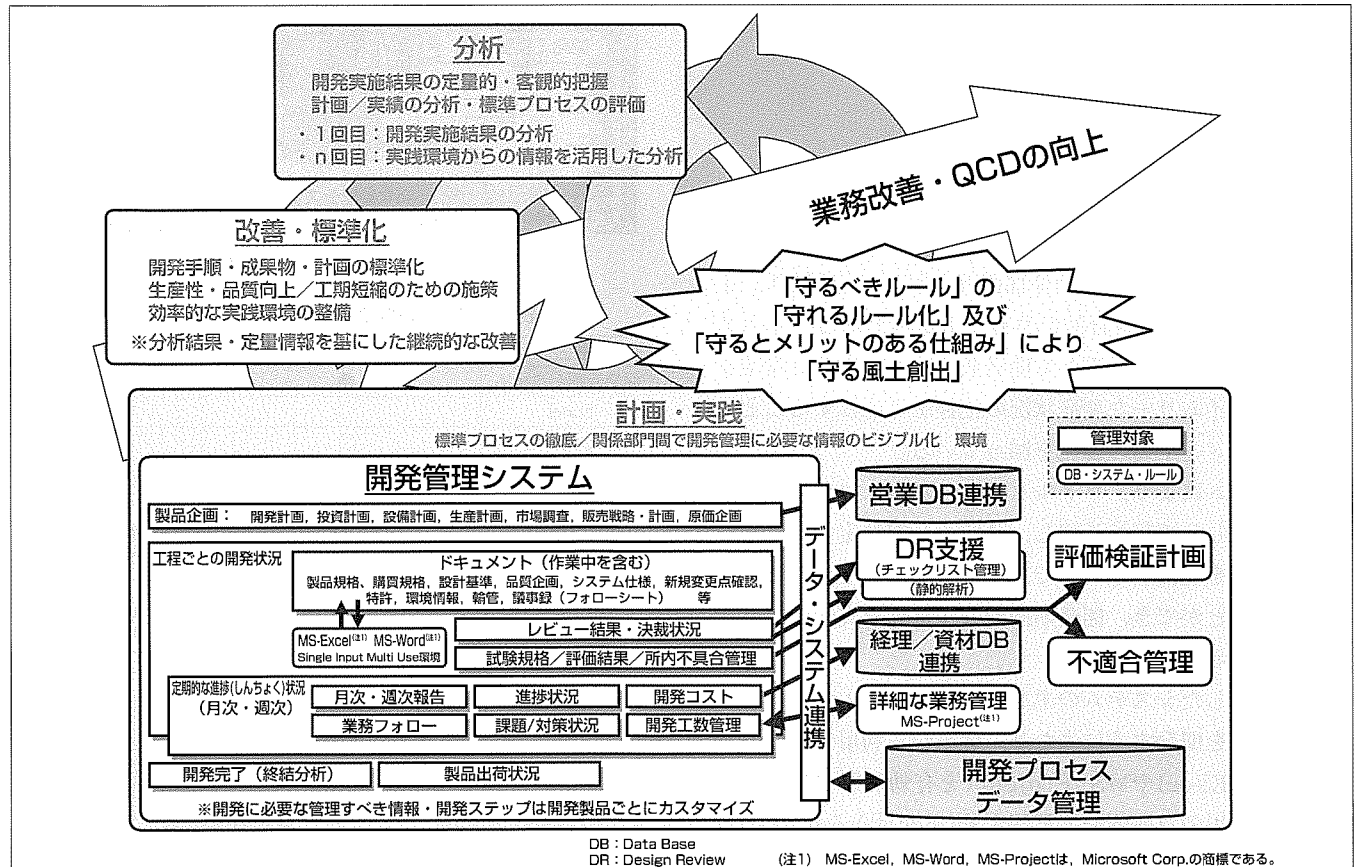
そこで、開発マネジメント力の強化により高品質の製品を短期間に開発することをねらいに、“開発の見える化”による開発フロントローディング活動を推進している。この活動の中で、製品開発における品質評価のタイミング(ホールドポイント)を中心に、開発状況と開発成果物を関係部門間(設計、品質管理、工作、その他部門)で統合的に共有する開発管理システムを開発した。

この開発管理システムにより、リアルタイムに見える化した情報を活用し、適切な段階での確な課題・問題点の早期特定と是正フォローが可能となり、開発の上流から品質作り込み(開発のフロントローディング化)による開発期間厳守・短縮を実現することが可能である。

また、この開発管理システムでは、設計レビュー結果等の開発成果物から開発管理に必要な情報を抽出し、開発状況に反映することで、開発管理にかかわる業務負荷の抑制を図っている。

本稿では、開発管理システムの概要と、システムを活用した開発フロントローディング活動、製品開発への適用方法等について述べる。

特集 II



QCD向上に向けた開発管理への取り組みと開発管理システム概要

開発管理への取り組み内容(①実業務の現状分析, ②開発プロセス改善・標準化, ③計画・実践環境の構築・適用とその継続)と改善の継続によるQCD(Quality, Cost, Delivery)向上について図示している。特に、計画・実践環境では、“開発の見える化”について、各工程で、開発状況と開発成果物を関係部門間(設計、品質管理、工作、その他部門)で統合的に共有する環境を表している。

1. ま え が き

近年、製造業では、世界的規模でのコスト競争の激化とともに、顧客要求に応じた高品質の製品を短期間に開発し市場に提供していくことが求められている。このような状況の中、製品開発の現場では、この要求を満足するため、開発マネジメント力の強化が切望されている。

従来の開発マネジメントは、現品会議等の品質評価のタイミング(以下“ホールドポイント”という。)で、関係部門(設計・品質管理・工作・その他部門)から紙資料で報告される開発状況や月次の開発進捗報告会等で行われていた。

このため、開発部門長や経営者を始め、開発当事者である関係者が開発状況をリアルタイムに把握することは困難であった。

そこで、開発マネジメント力の強化により高品質の製品を短期間に開発することをねらいに、開発の見える化による開発フロントローディング活動を推進している。

この活動を推進するために、下記、3項をねらいとした“開発管理システム”(以下“本システム”という。)を開発し、製品開発への適用及び機能拡張を図っている。

本稿では、開発したシステムの概要と、製品開発への適用方法及び適用効果等について述べる。

- (1) リアルタイムな開発状況の見える化
- (2) コンカレントな開発管理環境の整備
- (3) 開発管理業務の効率化

2. 開発管理システムの概要

本システムは、製品開発のホールドポイントを中心に、開発状況と開発成果物を関係部門間(設計、品質管理、工作、その他部門)で統合的に共有する環境である。本システムでは、作成中の段階から開発成果物を共有する環境を実現し、タイムリーな開発状況の把握を可能にすることで、開発マネジメント力の強化を図っている。

本システムにより、リアルタイム、かつ、コンカレントに見える化した情報を活用し、課題の早期特定と是正フォローの徹底を支援することで、開発をフロントローディング化することができ、開発期間厳守・短縮を実現することが可能である。

今回開発したシステムの主な機能を表1に示す。また、本システムを開発するに当たり、従来から利用しているツール(MS-ExcelやMS-Project)を有効活用することで、システム運用の負荷軽減と早期定着(早期見える化)を図っている。既存ツールの活用例を図1に示す。

また、表2に示すように、利用目的別に任意にツールを選択しても、同様の情報を得られる環境としている。

3. 製品開発への適用事例

3.1 開発管理システムの実現機能

3.1.1 開発状況の見える化

開発状況の見える化として、①ホールドポイントの実施状況の見える化、②日々の開発工程状況の見える化、③開発状況の分析、④品質状況の分析、について述べる。

(1) ホールドポイントの実施状況の見える化

図2は、本システムで管理している開発製品に対し設計

表1. 主な実現機能

実現機能	詳細
開発状況見える化	ホールドポイントの実施状況の見える化
	日々の開発工程状況の見える化
	開発状況の分析 品質状況の分析
開発成果物の管理	設計レビュー議事録、評価結果一覧表、課題・対策一覧表等の一元管理

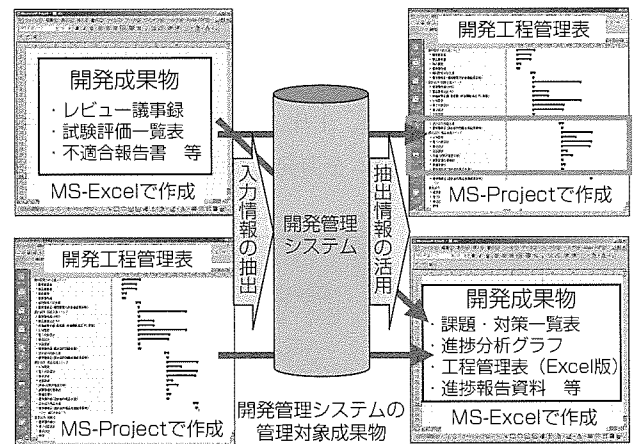


図1. 既存ツールの活用例

表2. ツール間での連携関係と主従関係

利用ツール	ホールドポイントの実施状況	日々の開発工程状況
開発管理システム	●	○
MS-Excel	○	○
MS-Project	○	●

●：入力先，○：活用先

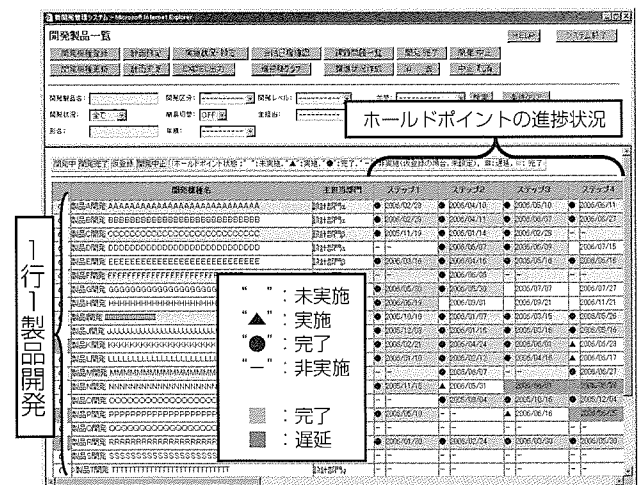


図2. ホールドポイントの実施状況の見える化画面例

レビューや製品評価会議等の品質評価ステップの実施状況を横断的に把握するための画面例である。

(2) 日々の開発工程状況の見える化

図3は、開発製品ごとに登録されたホールドポイントの計画工程と、MS-Excelで作成した評価結果一覧表の評価状況をMS-Projectに反映する機能イメージを示している。この機能により、以下の効果が得られた。

- (a) 開発工程の計画策定：設計作業に関する詳細な開発工程の計画策定の効率化
- (b) 開発工程の管理：設計の進捗状況と品質管理部門の評価状況の統合的な把握

(3) 開発状況の分析

図4は、本システムやMS-Projectで管理している工程計画と実績情報を定量化し、進捗評価のための分析グラフを作成する画面例である(図右上：EVA(Earned Value Analysis)グラフ、図下：初期の計画と最新の計画・実績の状況を横棒に示した表)。

この機能により、以下の効果が得られた。

- (a) EVAグラフ：開発日程の遅れの定量的な把握
- (b) 初期・最新計画と実績グラフ：計画の変更状況と

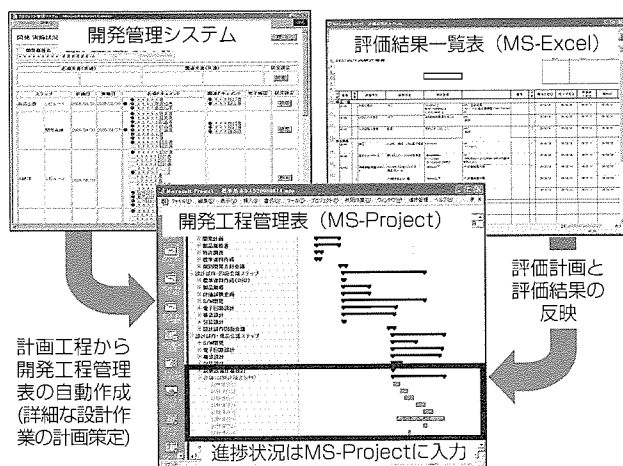


図3. 日々の開発工程状況の見える化機能イメージ

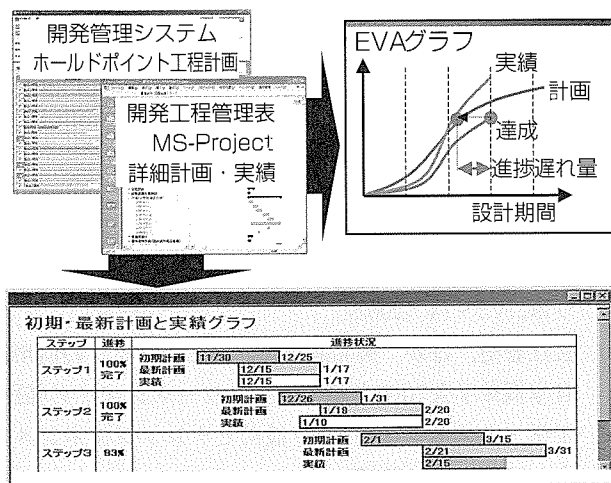


図4. 開発状況の定量的把握機能イメージ

計画と実績の差異状況、進捗遅れによる後工程への影響度の把握

(4) 品質状況の分析

図5は、MS-Excelで作成したレビュー議事録や品質不適合報告等から課題・問題点とその対策状況を抽出・一元管理し、対策状況をグラフ化したイメージ図である。

この機能により、以下の効果が得られた。

- (a) 課題・問題点、対策状況の一元管理：残課題の明確化と共有化。適切な漏れのない対策フォローの実践
- (b) 課題・問題点に対する対策状況グラフ：品質状況のトレンドグラフとして活用することで、課題の発生と改善状況を定量的に把握し、製品完成度を把握

3.1.2 開発成果物の管理

開発成果物の管理として、製品開発上でQCDに直接的にかかわる資料を、開発ホールドポイントと連携した形式で、作成中の段階から見える化している。

図6は、ホールドポイント別に、作成すべき開発成果物(設計レビュー会議・現品会議の議事録、不適合報告書、試験評価一覧表、課題・問題点対策一覧表、工程管理表、進捗報告資料等)を管理する機能イメージである。

3.2 製品開発への適用方法と適用手順

本システムは、三菱電機株福山製作所の製品開発に適用しており、以下の進め方で導入した。管理する開発分野はソフトウェア、機械構造、電気・電子回路等の全技術分野を対象とし、設計及び品質管理部門を巻き込んで導入検討した。導入手順を下記に示す。

- (1) 現状分析：実製品開発の手順、作成している開発成果物とその作成のタイミング、開発時の課題に対する対応状況の分析等を実施

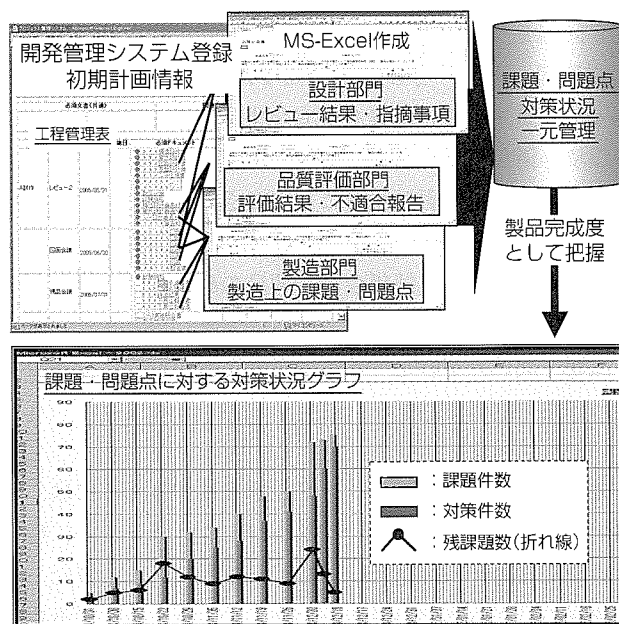


図5. 課題・問題点・対策状況の管理機能イメージ

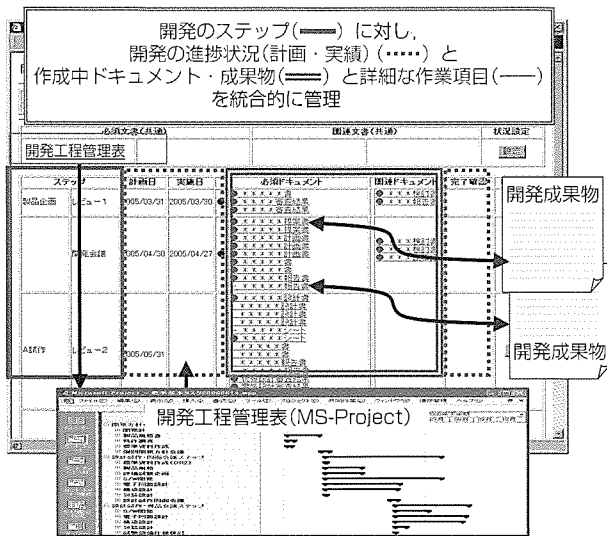


図 6. 開発成果物を管理する機能イメージ

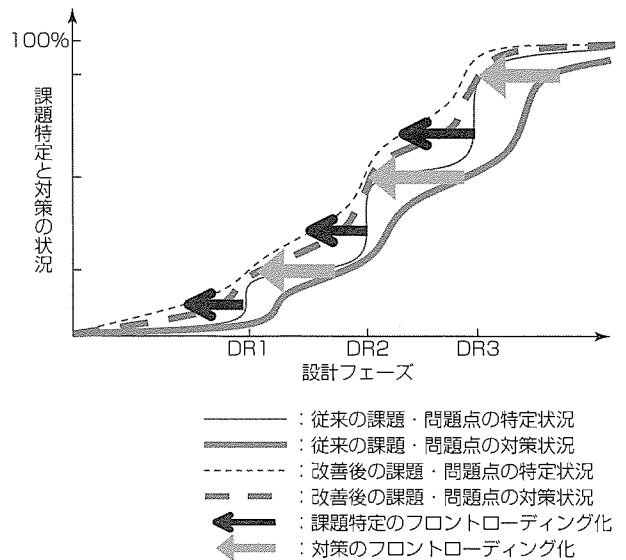


図 7. 課題特定と対策状況の推移

- (2) 開発プロセス標準化・改善：福山製作所の開発管理規則の再定義
- (3) システム開発・適用：再定義した開発管理規則を基に、福山製作所用の開発管理システムを開発し製品開発に適用している。なお、適用する製品は、重要機種については不可欠としている。
- (4) 継続した改善：福山製作所内保有システム(文書管理システム、設計レビューシステム、ソフトウェア障害表管理システム等)との連携等の機能強化活動を実施している。また、本システムに蓄積された見える化情報を定量的に分析し、次機種以降の開発業務改善に反映していく

なお、福山製作所では、上記(3)、(4)の継続的な改善活動を進めており、他製作所でも同様の活動を推進している。

4. 期待される業務改善効果

今回開発した“開発管理システム”の適用により、設計・品質管理・工作・その他部門間で、開発の進捗状況、課題・問題点・対策状況等を共有化する環境を開発した。この環境を活用することで、開発の上流から開発のフロントローディング化に貢献することができる。

図 7 に業務改善の一例を示す。従来は現品会議や設計レビュー会議等の品質評価会議で開発の課題・問題点を発見し改善していたが、このシステムにより、レビュー会議前に課題・問題点を特定する等の業務革新が可能になった。

5. む す び

開発のフロントローディング化を実践するためには、的確な開発状況をリアルタイム、かつ、コンカレントに把握する環境(開発情報の見える化)が不可欠である。また、開発情報の見える化を実現するためには、見える化するため

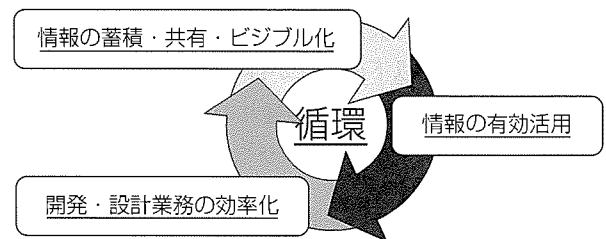


図 8. 開発情報の見える化に必要な循環

の情報を効果的に収集する必要がある。

今回、開発マネジメント力の強化活動の一環として、開発情報の見える化に必要な循環(図 8)を考慮したシステムを開発し、製品開発への適用を開始した。

以上、開発マネジメント力に着目し①リアルタイムな開発状況の見える化、②コンカレントな開発管理環境の整備、③開発管理業務の効率化、について開発したシステムを適用事例とともに述べた。

この開発管理システムを製品開発のためのフロントローディング環境と位置付け、開発状況の見える化を促進していくことで、製品開発の短期間化・品質向上に寄与できると考えている。今後も、継続した業務改善を推進するとともに、当社内に適用を拡大していく所存である。

参 考 文 献

- (1) 長江雅史, ほか：製品開発管理システムの開発・適用による設計効率化, 精密工学会 第20回設計シンポジウム, 72~74 (2002)
- (2) 長江雅史, ほか：製品開発におけるナレッジの活用, 日本機械学会2005年度年次大会ワークショップ(設計工学・システム部門企画) 設計とナレッジマネジメント, 355~356 (2005)

社会インフラシステム開発におけるソフトウェア開発プロセス改善

安江 悟* 田中隆行†
 風間由美子**
 川端達明***

Software Process Improvement in Social Infrastructure Systems Development

Satoru Yasue, Yumiko Kazama, Tatsuaki Kawabata, Takayuki Tanaka

要 旨

社会インフラシステムは、大規模化・複雑化している一方で、国内電力・公共市場の設備投資抑制、経費削減の継続による顧客の価格低減要求と市場競争の激化による価格の下落、及び納期の短縮化が急速に進んでいる。市場競争力の維持・強化のためには、ソフトウェアの開発効率化、及びロスコスト削減が不可欠になっている。

このような背景から、三菱電機では、ソフトウェア品質向上と開発効率化をねらいに、ソフトウェア開発プロセス改善活動を開始し、現場のヒアリング・分析結果を踏まえて以下の3つの取り組みを実施した。

(1) ソフトウェア仕様の見える化による手戻り削減

UML(Unified Modeling Language:統一モデリング言語)を用いてソフトウェア仕様をビジュアル化することで、仕様レビューを効率化し、分析・設計段階での誤り混入を防止し、手戻りを削減した。

(2) コーディング規約+静的解析による手戻り削減

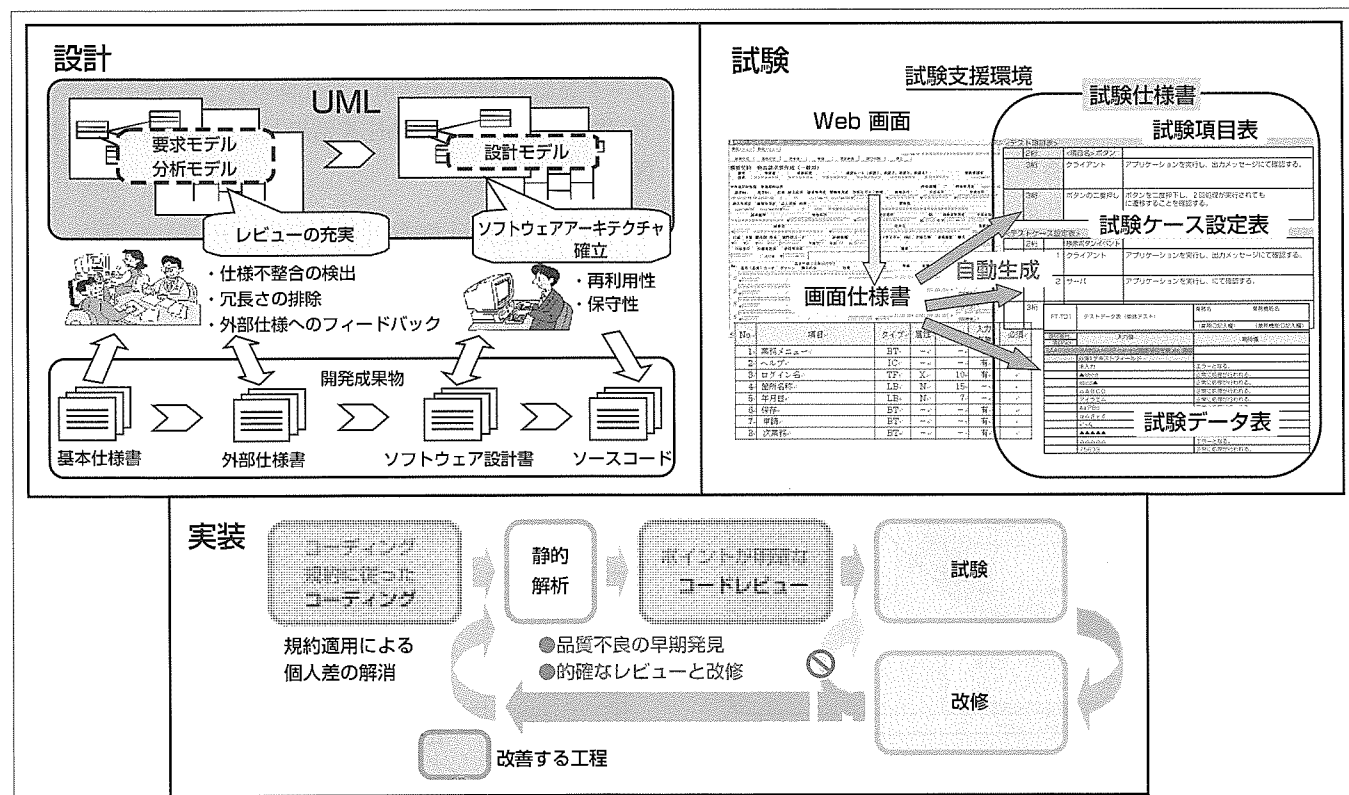
静的解析技術を活用してコーディング規約違反を効率的に検出し、かつプログラム品質を見える化(=定量化)する環境を構築することで、実装段階での誤り混入の防止と品質向上を図り、手戻りを削減した。

(3) Web系システム向け試験支援環境構築による試験工数削減と品質向上

試験仕様書生成の自動化及び試験品質の均一化を目的に試験支援環境を構築し、多数の画面を持つWeb系システムの品質を維持しつつ膨大な試験工数を削減した。

以上の取り組みにより、社会インフラシステム開発において、ソフトウェアの見える化が定着し、開発効率化、品質向上を実現した。

本稿では、以上の3つの取り組みの目的、実施内容、効果について述べる。



開発効率化、ロスコスト削減のための3つの施策

設計/実装ではソフトウェアの見える化による誤り混入防止、試験では試験の効率化に取り組んだ。①設計では、UMLを活用してモデリングを行うことで仕様見える化し、レビューを充実、②実装では、コーディング規約と規約を徹底させるため静的解析技術を活用し、コードレビューを充実、③試験では、試験仕様書生成の自動化など試験支援環境構築により試験を効率化した。

1. ま え が き

社会インフラシステムは、大規模化・複雑化が進む一方で、市場競争の激化による価格の下落、短納期化が急速に進んでいる。市場競争力の維持・強化のためには、ソフトウェア開発の効率化、ロスコストの削減が重要な課題になっている。これら課題解決のため、当社の社会インフラ事業部門では、ソフトウェア開発プロセスの改善組織を作り、ソフトウェアエンジニアリングを中心にプロセス改善活動を行った。まず初めに、現状の課題を分析の上、以下の3項目に重点を置いて活動を行った。

- (1) ソフトウェア仕様のレビューを十分にを行い、仕様設計段階での誤り混入を削減
- (2) コーディング規約違反検出の効率化、プログラム品質の見える化(=定量化)を実施し、実装段階での誤り混入を削減
- (3) 大規模Web系システムの膨大な画面試験工数を削減

2. ソフトウェアプロセス改善活動のねらいと組織

2.1 プロセス改善活動のねらい

市場価格低下に対応し、社会インフラ事業のソフトウェア部門全体の開発効率化と品質向上をねらいに、ソフトウェアプロセス改善活動を開始した。活動の基本方針は、①共通課題の改善、②標準化、③技術の横通しとし、設計/実装/試験品質の改善と、仕様/実装品質の見える化、試験の効率化に取り組んだ。活動のねらいと概要を図1に示す。

2.2 ソフトウェアプロセス改善の推進体制と展開

プロセス改善組織は、社会インフラ事業部門のプロセス改善実施部門と、各部門の代表、ソフトウェア開発協会の代表で構成した。また、開発プロセス改善を担当する本社技術スタッフ(設計システム技術センター)が活動を支

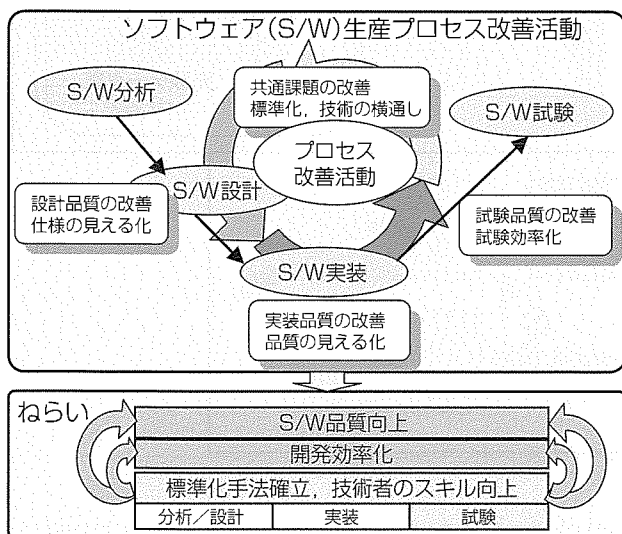


図1. 活動のねらいと概要

援し、これまでのノウハウの水平展開により活動を加速化した。

3. ソフトウェアプロセス改善内容

プロセス改善実施に先立って開発効率化と品質向上を実現するためにソフトウェア開発部門の現状調査を行った結果、①プロジェクト崩れの防止、②手戻り工数の削減、③生産性の向上、が課題として抽出された。これらの課題の解決のためには、設計のフロントローディング化による開発の上流での品質作り込みが有効であるという判断から、ソフトウェア仕様見える化とプログラム品質見える化をキーワードに、ソフトウェア開発部門全体の風土改革を行うことにした。

一方、大規模Web系システムの画面と画面を構成するフィールドの入出力試験には膨大な時間を要するために、品質を維持しつつ試験時間を短縮する施策を実施した。

3.1 ソフトウェア仕様見える化

当社の社会インフラ事業のソフトウェア開発では、設計から実装までの工程は、製作フェーズによる分業化が進み、ソフトウェアの要求仕様を明確に提示できる技術が重要になっている。また、あるプロジェクトの試験段階で検出された誤りの分析結果では、前工程の理解不足による誤りが全体の59%を占めており、ソフトウェア仕様を正しく伝えることが手戻りを削減する上で最も効果的であった。そのため、ソフトウェア仕様見える化し、レビューを効率化する技術として、グローバルスタンダードである統一モデリング言語(UML)を活用した仕様見える化(=モデリング)技術を導入した。UMLを活用した仕様記述イメージを図2に示す。

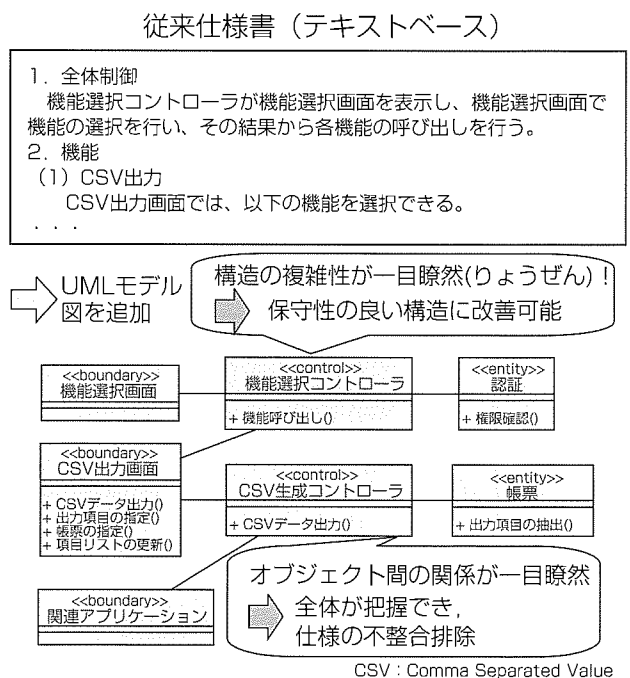


図2. 見える化技術による仕様記述イメージ

3.1.1 ソフトウェア仕様の見える化技術の導入

UMLを活用したソフトウェア仕様の見える化技術の導入・適用は図3の手順で行った。まず、適用プロジェクトに対して、開発手順と成果物を規定し、業務分析/要求分析/システム分析/設計手法を明確化した。その上で、UMLを活用した分析・設計モデルのサンプル作成、モデルの作り方の説明、モデル作成/修正とレビューを繰り返し、分析・設計フェーズでの仕様の見える化技術を教育し実践した。適用した開発手順とドキュメント体系については、見直し/整理、及び標準化を行い、開発ガイドラインとしてまとめた。ガイドラインの作成に当たっては、社内で蓄積されたUML適用ノウハウを反映するとともに、グローバルスタンダードを意識し、SLCP(Software Life Cycle Process)に準拠させた。開発ガイドラインにより、他プロジェクトへの仕様の見える化技術の短期導入を可能とした。

3.1.2 ソフトウェア仕様の見える化技術の展開

見える化技術の展開、定着化のため3つの活動を行った。

第1に、活動の効果を関係者に理解してもらうために、ソフトウェア品質計算方法を策定し、効果算定シートの作成を行い、品質と効果を見える化した。

第2に、若手によるUML研究会で、UML技術を活用したWebシステムの共通基盤の勉強会、適用事例研究を行い、今後の展開の中核メンバーを立ち上げた。

第3に、次の各種教育を実施した。①全ソフトウェア設計者を対象に、全体的な技術力を向上するためのUML基礎教育、②中核技術者を対象に、見える化技術の実践力を養成するための演習に重点を置いた分析/設計段階のモデリング手法教育、③管理者を対象に、見える化技術をトップダウンに推進するための管理者の視点でのUML入門教育。

3.1.3 効果

同規模の類似システムでは、“前工程の理解不足”に起因する誤りが試験段階で検出された誤りの59%を占めていたが、ソフトウェア仕様の見える化技術の適用により0件になるとともに、試験段階での誤り指摘件数が半減した。また、現在、提案段階でのシステムの要求分析にも適用しており、従来であれば試験するまで検出できなかった不整合や誤りが検出でき、有効性が確認できた。

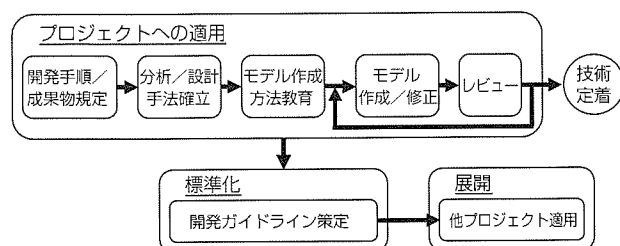


図3. 見える化技術導入、適用手順

3.2 コーディング規約+静的解析による品質向上

製品品質に直結するプログラム品質を向上させることが重要で、そのためには、プログラム作成者の技術力向上、プログラム品質の見える化(=定量化)が必要不可欠であり、CとJavaを対象に、以下の取り組みを実施した。

- (1) コーディング規約の作成
- (2) コーディング規約違反の効率的な検出(静的解析)とプログラム品質の見える化(=定量化)
- (3) プログラム受入れ基準の策定と義務化

3.2.1 コーディング規約の作成

全体的なプログラム品質向上及びコードの属人性を排除するために、コーディング規約を作成した。従来の命名規則中心のコーディング規約に誤りが混入しにくいコードを作成するための実装規則を加えるとともに、全社で蓄積していたノウハウの反映を行った。

3.2.2 コーディング規約違反の効率的な検出(静的解析)と品質の見える化

コーディング規約を守らせるために、静的解析環境を整備した。静的解析ツールは、出力する警告が多すぎるため、ツールが出力する警告のレベル分けを行い、欠陥に直結する不具合を効果的に修正できるようにした。作成したコーディング規約とともに、静的解析技術及び静的解析の環境について、プログラミング技術者を対象に教育を行った。これにより、開発者に技術を浸透し、静的解析技術の運用を加速した。実装段階の不具合流出を防止するため、実装プロセスを図4のように改善し、新規作成/修正するたびに、静的解析結果を利用して効果的なコードレビューを行うようにした。

次に、上記活動の定着とプログラム品質の見える化(=定量化)を目的に、静的解析環境が出力する重要警告及びメトリクスの選定を行い、解析結果を収集・蓄積する環境を作成した。図5は解析結果のレポート例である。このレポートを利用して、個々のプログラム品質はもちろんのこと、部門のプログラム品質レベルや傾向、品質改善状況などを定量的に把握可能とした。

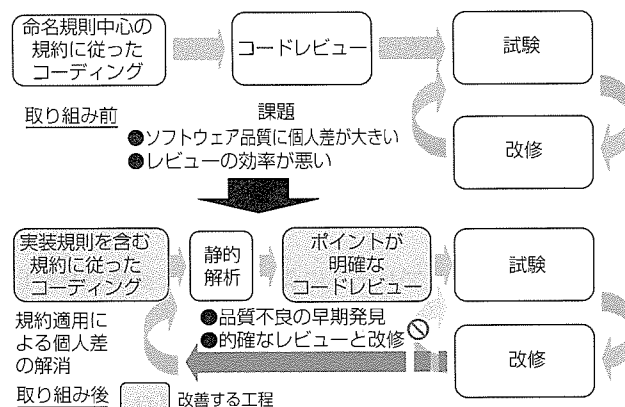


図4. 実装プロセスの改善

プログラムの 数	静的解析 リスク率	プログラムの 平均	静的解析結果 (平均)			プログラムの 平均		
			最大値	推奨値	推奨値を 超えた数	最大値	推奨値	推奨値を 超えた数
63	3.6	37.2%	231	17.16%	4690000	3	1.15%	
138	29.5	47.3%	764	3.1230%	97	5	6.00%	
34	1.1	34.3%	29	14.230%	6000000	2	1.50%	
25	5.4	45.5%	19	5.15%	4690000	10	1.15%	
93	52.4	34.2%	192	0.60%	13	2	0.80%	
72	3.4	22.4%	854	3.1421%	55	0	1.15%	
29			181	23.52%			14.15%	

図5. 静的解析集計のイメージ

3.2.3 プログラム受入れ基準の策定と義務化

ソフトウェア製作部門開発のプログラム受入れ時に、図6のような静的解析レポートの納品を義務付けるとともに、プログラムの受入れ基準を明確化した。具体的には、重要な約20個の警告、メトリクスに対して基準値の設定を行い、条件を満たさない場合は、受入れ不可とする運用を決めた。併せて、静的解析レポートの納品を明記できるように、受入れシステムを変更した。

3.2.4 効果

各部門に対するコーディング規約と静的解析環境の整備による規約遵守を徹底した結果、以下の効果が得られた。

- (1) 実装時の不具合混入の防止により手戻り工数を削減
- (2) コーディング規約遵守によりプログラム品質を向上
- (3) メトリクス値を用いプログラム品質の定量化を実現
- (4) 警告により単純ミス削減しプログラム品質を向上

3.3 Web系システムの試験支援環境構築

大規模なWebアプリケーションでは画面数が多く、画面仕様に基づく境界値試験の試験工数削減が重要となる。試験対象となるJava, JSP (Java Server Pages) (注1) コードに対してはチェックツールの組み込みなどによりバグを低減する手法がとられる。しかし、納品時の試験が不要になるわけではなく、客先納品物としては画面仕様に基づいた試験が実施されていることを示す試験成績書は不可欠である。

特に試験設計では、個々の画面及びその中に含まれる多数のフィールドに対して試験項目を考案することは非常に手間のかかる作業であり、試験項目漏れも起こしやすい。

画面仕様にかかわる試験表の作成時間の低減及び画面仕様に対する試験項目の漏れ抑止を目的に、Webアプリケーション (Java, JSP) の試験仕様書生成ツールを開発した。

3.3.1 試験仕様書生成ツールの開発

図7に試験仕様書生成ツールの概要を示す。開発した試験仕様書生成ツールが持つ機能は以下のとおりである。

- (1) 画面仕様に基づいた試験表 (試験項目表, 試験ケース表, 試験データ表) をテンプレートとしてパターン化する。
- (2) 画面仕様とテンプレートにより基本的な試験項目を自動生成する。

3.3.2 効果

これまでに、試験仕様書生成ツールを5プロジェクトに

(注1) Java及びJSPは、Sun Microsystems, Inc.の登録商標である。

基礎データ項目	データ
ファイル数	9個
ヘッダーファイル	0個
その他	個
コード総行数	4954行
コード総行数(コメント除く)	3354行
実行コード行数(宣言文除く)	1826行
定義された関数	57個
関数リファレンスの総数	412個

ソースコード特性	測定(最大値)	推奨値	推奨値を超えた数
未初期化変数(個数)	10	0	—
メジャーな警告の割合	72	—	—
明瞭な関数宣言のリスク率	23.06	9.5	—
コメント率	32.30	30	—
テスト性(静的検査)	46825240	200	14
ネストの深さ	9	7	1
マイケースインターバル	22	10	4
サイクルマテック複雑度	48	20	7
1関数内に含まれる行数	287	200	4
1ファイルあたりの関数数	20	50	0

図6. 静的解析レポートのイメージ

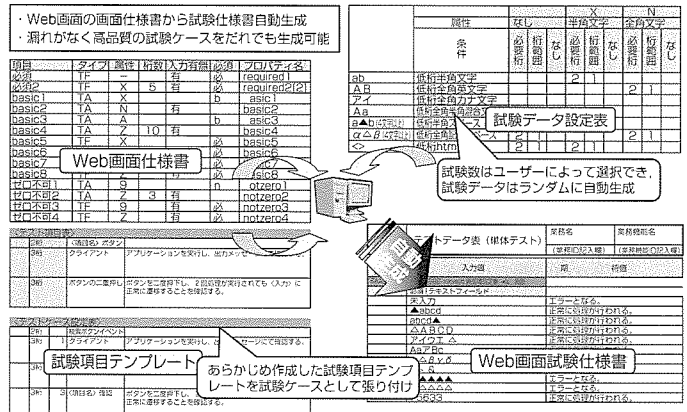


図7. 試験仕様書生成ツールの概要

適用し、以下の効果が得られた。

- (1) 仕様書の自動生成により、試験計画時間の8割を削減
- (2) 画面標準仕様に合致し漏れのない試験項目の抽出により、試験品質のばらつきを抑制
- (3) 試験入力データの自動抽出により、入力条件が画一化され、試験網羅率が向上

4. む す び

これまでに述べた活動により、ソフトウェア仕様とプログラム品質の見える化を行う風土を作り、開発効率化と品質向上を達成した。今後は、これら施策の更なる展開とともに、改善効果の適切な把握と計測結果をソフトウェア開発プロセスの改善にフィードバックすることを目的に活動を進めていく。そのため、ソフトウェア開発の進捗(しんちよく)や品質を定量的に計測する仕組み、及び組織を更に強化する。また、この取り組みは、社会インフラ分野に限らず、他の事業分野に対しても重要な取り組みであり、広く水平展開を推進する予定である。

戦略的再利用に基づくソフトウェア開発

小島泰三*
辰巳尚吾**
原内 聡**

Strategic Software Reuse

Taizo Kojima, Shogo Tatsumi, Satoshi Harauchi

要 旨

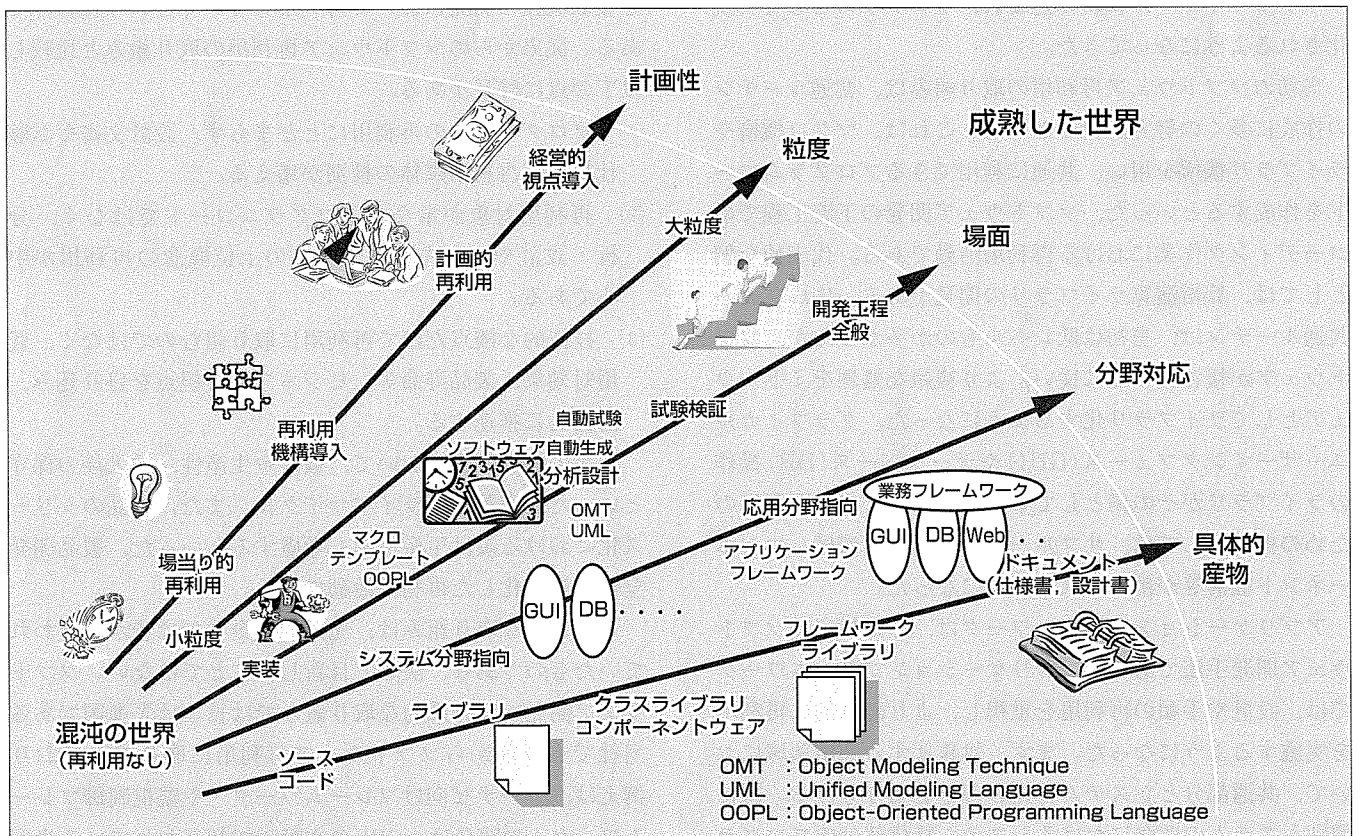
戦略的なソフトウェア再利用手法として、ソフトウェアプロダクトライン(SPL)によるアプローチが注目されている。既に各社からSPLに準じた試みが多数報告されており、その効果も確認されている。SPLによるソフトウェア再利用は、オブジェクト指向プログラミングや分析設計手法といったソフトウェア再利用技術自体に重点を置いたものではない。従来の再利用技術の導入と比較し、より大きな粒度でのソフトウェア開発効率の向上をねらっている。

戦略的なソフトウェア再利用は、再利用活動の成熟により到達されるものである。この手法が強調するのは、個々の再利用技術ではなく、その運用や再利用への取り組み姿

勢である。この手法で利用される再利用技術は、特に目新しいものではなく、既に確立されたプログラミング技術や分析設計手法である。それら技術の運用において、まず対象製品について、性能や機能等の性質だけでなく、製品寿命や実現に使われる個別技術の動向についても考慮する等、体系的に対象領域を整理する。そして、何をどう再利用すればどの程度の効果が上がるかを考慮した上で取り組むことが、この手法の根幹をなしている。

本稿では、まずソフトウェア再利用の変遷と戦略的ソフトウェア再利用について概要を述べ、次に、三菱電機における取り組み事例について述べる。

特集 II



ソフトウェア再利用活動の成熟

ソフトウェア再利用活動は、その成熟度に従い、実施形態、再利用の粒度、どのような活動において再利用されるか、どのような分野を対象とするか、そして、具体的産物に変化する。再利用のない状態から、場当たりに流用される段階を経て、再利用機構を用いた現場レベルの活動、次に計画性を持った活動に変化する。今日のSPLのような戦略的再利用では、計画性に加え、更に経営的視点を導入した全体最適が試みられている。

*先端技術総合研究所(工博) **同研究所

1. ま え が き

ソフトウェアプロダクトライン(SPL)⁽¹⁾は、戦略的な再利用に基づくソフトウェア開発方法論である。従来からのソフトウェア再利用の取り組みと比較し、ビジネス的な視点を強く取り込み、計画的に進めていることに特長がある。

本稿では、戦略的なソフトウェア再利用について概要を述べ、その具体例として、当社で現在進めている衛星地上局システム対応と列車統合管理装置対応の取り組みについて述べる。

2. 戦略的再利用

2.1 再利用の変遷

ソフトウェア再利用の取り組みは、その成熟とともに、偶然の産物から計画的な活動に、ボトムアップからトップダウンでのアプローチに、そして開発工程に関しては、下流工程から上流工程を対象としたものに移り変わる。例えば、プログラムだけでなく、設計文書や試験手順書等の多種多様なものが、再利用を通じて生産されるようになった。また、再利用されるものは、たとえ再利用の産物がプログラムであったとしても、単なるプログラムコードの断片だけでなく、分析や設計結果、さらには手順といったものが、ライブラリやツールに組み込まれ、プログラムとして具現化されるようになってきた。

当初のソフトウェア再利用の取り組みは、共通ルーチンの作成に多くの努力が費やされた。これは、マクロ機構やライブラリ機構を用い、共通に利用できるプログラムコードを作成するといった、ソフトウェア開発の下流工程でのコーディング作業における再利用活動である。代表的な例としては、算術演算ライブラリの開発がある。作成される共通ルーチンは、当初は低レベルものが多かったが、ソフトウェアが複雑化するに従い、より複雑な処理をミドルウェアとしてライブラリ化するようになった。グラフィカルユーザーインタフェース(GUI)やデータベース(DB)操作のライブラリがその例として挙げられる。また、再利用のための機構としては、サブルーチンやクラス機構、コンポーネント機構等が用いられるようになった。

アプリケーションフレームワークは、分野指向のソフトウェア開発手法である。アプリケーションフレームワークでは、設計や手順の再利用を重視し、より計画的に再利用を実施するようになった。まず、対象とする問題領域において、共通部分とシステム特化の部分とを切り分ける。次に、個別システムの開発におけるシステム特化部分のプログラムや定義情報の作成手順をあらかじめ設定し、これを支援する分野特化のライブラリやツールの提供等を用意する。コードレベルの再利用にとどまらず、ライブラリやツールに組み込まれた分析結果や設計情報を再利用することで、

より大規模で効果のあるソフトウェア再利用が達成される。

モデル駆動アーキテクチャ(MDA)^{(2)(注2)}がソフトウェア再利用と関連付けられて語られる場合がある。MDAでは、対象領域を機械処理可能な形式でモデル化し、このモデルから実行可能なソフトウェアを実現する。MDAの貢献は、モデル化をする意義を明確にし、その作業を啓蒙(けいもう)したことにある。ソフトウェアの仕様を正確に記述することは、ソフトウェア品質に対する意義が大きい。一方、MDA単独では、ソフトウェア再利用に対して、効果は薄い。しばしば抽象的なモデルにより再利用性が向上されると言われるが、オブジェクト指向方式のクラスの利用と同様、再利用可能な形式で適切にモデル化できた場合に限られる。現状のUMLベースのMDAでは、再利用のための機構が不十分であり、単独でソフトウェア再利用の効果を上げることは難しい。MDAでも、他の取り組みと同様、分野指向の取り組みと組み合わせることで、再利用を向上させる取り組みが行われている。

2.2 経営的視点の導入

現在、ソフトウェア再利用に対する体系的な取り組みが注目されている。SPLでは、一連の製品群の開発において、機種間で共通に利用できるプログラムライブラリや試験環境などの資産をあらかじめ“コア資産”として構築し、それを複数機種の開発において再利用していくという枠組みである。従来からのソフトウェア再利用の取り組みと比較し、以下の点に特長がある。

- (1) プログラムでの再利用にとどまらず、設計文書や試験仕様等、再利用媒体の種別が増える。
- (2) 再利用対象が単なるプログラムコードではなく、分析・設計やアーキテクチャ等の上位概念の再利用が中心である。
- (3) 技術的な観点だけで再利用に取り組むのではなく、費用対効果、製品寿命等、ビジネス的な視点を盛り込み、計画的に推進する。

製品の設計段階において、機能や生産性、納入後の保守といった個別製品のライフサイクル、また、製品のシリーズ化における設計生産体制も考慮するといった、製品開発全体で最適化した再利用活動である。

このような取り組みは、先進的な企業では昔から行われていたものであり、決して目新しいことではない。ソフトウェア開発への体系的な取り組みでは日本は先進国である。当社でも以前からソフトウェア再利用に取り組んでおり、例えば、カーナビ向けフレームワーク⁽³⁾や監視制御フレームワーク⁽⁴⁾の開発は、SPLの文献(1)で紹介されている米国での事例と比べても遜色(そんしょく)のない成果を上げている。今日、戦略的な再利用の取り組みが注目を受けているのは、①携帯電話やカーナビ等の高機能化によりソフト

(注2) MDAは、Object Management Group Inc.の登録商標である。

ウェアが大規模で複雑になったこと、②そのソフトウェア障害の与える影響は社会規模となること、③ソフトウェア開発コストや不具合による改修コストが企業経営を圧迫するようになったことによる。また、各社による取り組みがSPL等という名前で分類され、紹介されることで広く世の中に知られるようになったことも影響している。

戦略的なソフトウェア再利用が有効に働くためには、その活動に対する経営層の認知と支援が必要である。従来は、現場レベルに閉じたボトムアップな再利用や、コードレベルでの再利用が中心であった。これに対し、製品開発全体で最適化した効果の大きい再利用活動とするには、部門をまたがる連携や業務プロセスの変革を必要とする場合がある。既に経営層は、ソフトウェア開発効率化に対する取り組みの必要性を、現実のソフトウェア開発に要するコストから必然的に理解できているものと考えられる。したがって、戦略的な取り組みによる投資と回収を経営層が理解できる形で示し、支援を得ることができるかどうか成功の鍵(かぎ)となる。ただし、取り組み後の全体イメージの提示だけでなく、部分的に着手し、成果を段階的に示せる仕組みも考慮すべきである。

3. 事例紹介

一般にソフトウェア再利用の取り組みは、再利用の産物と対象をプログラムコード以外にも展開することで、より高度な再利用へと成長する。戦略的再利用においても同様である。活動の進展や環境変化に伴い、課題の重みが変わり、また、新たな課題が見付かる。以下では、筆者らが進める継続的な再利用活動について述べる。

3.1 衛星運用プロダクト作成支援

衛星システムのソフトウェアは、衛星搭載と地上系のソフトウェアに大別される。このうち、地上系ソフトウェアには、追跡管制システムや衛星シミュレータ等のプログラムモジュールのほか、衛星運用時に用いるハンドブックや運用手順書等の文書類が含まれる。これら文書類は、衛星運用プロダクトと呼ばれ、衛星打ち上げ前の運用準備作業の中で整備され客先に納入される重要な物件である。

衛星システム全体の開発では、追跡管制システム等のプログラムや定義データだけでなく、運用プロダクトの作成効率化も有用である。衛星追跡管制システム“BirdStar”⁽⁴⁾におけるソフトウェア再利用の産物は、ソフトウェアモジュールと当該ソフトウェアが用いる定義データである。運用プロダクトの作成は、BirdStarの範囲外であり、その作成においては、衛星システムの信頼性確保のため、内容や整合性の確認に多大な労力を要する。一方、運用プロダクトの作成には、高度な知識と経験が要求され、対応できる人員に限りがある。そこで、BirdStarの開発と並行し、これら文書類作成の枠組みについての検討に着手した。

図1に、この取り組みにおける処理の流れを示す。図のように、衛星システム開発における定義情報は、衛星の源泉情報を基に作成する各種定義ファイルや文書類から構成される。衛星運用における定義情報には手順情報や時系列のイベント情報が含まれるが、これらは、衛星ごとに大きく異なることはなく、共用化が可能である。一方、運用手順書や詳細運用フローは、使用する定義情報が同じでも、納入先、又は衛星ごとに文書レイアウトが異なることが多い。そこで、文書の論理構造とレイアウトとを分離し、衛星ごとの運用手順書や詳細運用フローの作成では、論理構造に表示スタイル情報を組み合わせて自動生成する枠組みを導入する。論理構造部の作成手順は安定し、対象衛星が変わっても、同様の手順で作業できる。このため、共通に使える作成支援ツールの導入が可能となる。また、同一の論理構造に対し、異なる表示スタイル情報を組み合わせる等、論理構造自体の流用性も向上する。図2は、開発した詳細運用フロー作成ツールの画面例である。このツールは、運用フロー論理構造の編集系であり、作成された論理構造を基に、画面表示や印刷等の用途に合わせ、フロー図を自動生成する。

現在、この枠組みの実現性について評価検討中である。これまでに、衛星運用ハンドブック生成ツールや詳細運用フロー作成ツール等の、枠組みの一部となるツールを開発

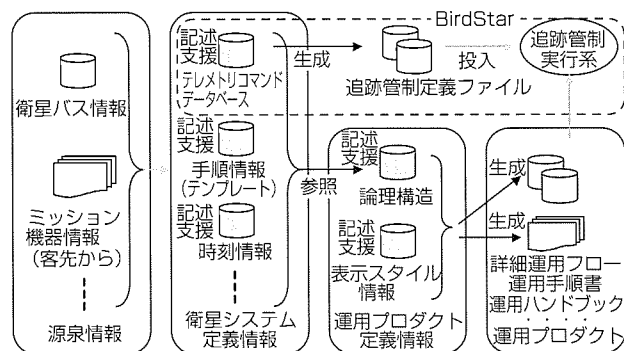


図1. 衛星運用プロダクト構築環境

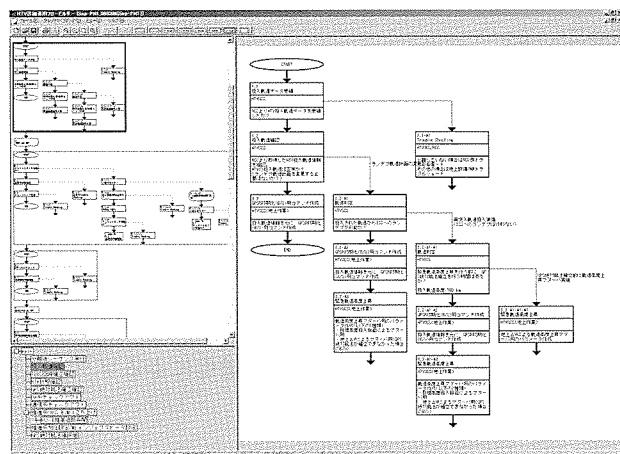


図2. 衛星詳細運用フロー作成ツール画面例

し、実システム開発に供することで、その有効性の確認を行っている。

3.2 列車統合管理装置システム試験環境

列車統合管理装置 (TIMS) は、列車に搭載される機器全体を監視制御する分散組み込みシステムである。TIMSは、製品間の機能の類似性が高いものの、列車の構成、機器や列車運用の多様性から、従来、ソフトウェアを毎回作成する必要があった。近年、TIMSに搭載する機器や実現機能の多様性が増大しており、従来の開発方法では、生産性や品質維持コストが問題となっていた。これに対応するため、SPLに基づくTIMSソフトウェア開発を実施した⁽⁵⁾。この開発において、まず、プログラムモジュールを対象に部品化とその合成ツールの開発に注力し、その後、システム試験環境の開発に重点を移した。

TIMSのソフトウェアの個別機種開発における変動要因は、主として列車構成にある。列車構成に応じてTIMSユニットが保持するデータやユニット間の伝送パケットが変化し、これを扱うためのプログラムコードを自動生成する。システム試験に対しては、再利用されるアルゴリズムに関連付けた抽象的な試験仕様を列車構成に基づき具体化することで、試験仕様を自動生成する(図3)。

図4にシステム試験実行環境の概要を示す。システム試験実行環境は、機器エミュレータと、それらの伝送を制御する試験実行ツールから構成される。試験実行ツールは、①与えられた試験仕様に従って機器エミュレータに動作を指示する。次に、②機器エミュレータが収集したTIMSユニットの出力を取得し、それを③試験仕様に記述された期待値と照合して試験結果を判定する、という手順で試験を実行する。一連の試験実行において、人手操作が不要となり、人為的ミス削減できることにより、コスト低減、及びソフトウェア品質の向上に貢献する。

現在、試験仕様の自動生成機能について、実用性を考慮しながら検討を進めている。並行して、システム試験実行環境をTIMSの一部機能のシステム試験に適用中であり、使用者からの意見を反映し、適用範囲の拡張に向け開発を進めている。

4. む す び

本稿では、戦略的ソフトウェア再利用について、その概要と事例を述べた。戦略的ソフトウェア再利用の考え方は新しいようで、その取り組みは古くからのものである。SPLといった言葉を用いることなく、これまでに様々な取り組みが進められている。本質は、ソフトウェア開発において、経営的視点も含めた、全体最適化によるソフトウェ

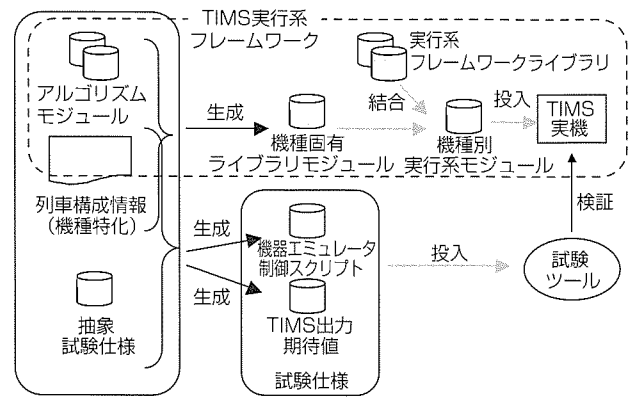


図3. TIMS試験仕様自動生成

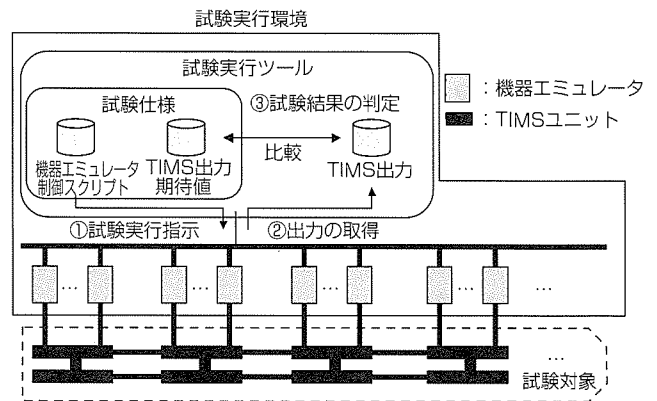


図4. TIMSシステム試験実行環境

ア生産性、品質の向上を達成することである。一方、その具体化のためには、経営層からのトップダウンによる指示が必ずしも必要ではなく、現場レベルでも、段階的に、そして、着実に取り組むことでも達成できる。重要なことは、全体構想を持ち、その中での位置付けを意識しながら進めることである。

参考文献

- (1) Clements, P., et al.: Software Product Lines, Addison-Wesley (2002)
- (2) Frankel, D.S.: MDA™モデル駆動アーキテクチャ, SIB ACCESS (2003)
- (3) 草間利樹, ほか: カーナビゲーションソフトウェア開発環境, 三菱電機技報, 74, No.9, 595~598 (2000)
- (4) 小島泰三, ほか: 監視制御システム向けフレームワーク, 三菱電機技報, 77, No.7, 451~454 (2003)
- (5) 吉田 実, ほか: 列車情報管理装置のソフトウェアプロダクトライン, 三菱電機技報, 77, No.7, 479~482 (2003)

カーナビ開発における フロントローディング型実装設計

小林 孝* 山中康弘***
船場裕次** 堀越美香***
片岡秀康†

Front Loading Design of Car Navigation System

Takashi Kobayashi, Yuji Funaba, Hideyasu Kataoka, Yasuhiro Yamanaka, Mika Horikoshi

要 旨

デジタル技術やネットワーク技術を融合した携帯情報機器、カーナビゲーションシステム、情報家電などは、日本が世界をリードする製品分野として期待されている。これらの分野では、多機能化や高性能化により製品競争力を高めるために、システム規模の拡大と動作周波数の高速化が進んでいる。近年、三次元CAD(Computer Aided Design)の干渉チェック機能を駆使して高精度な公差設計により、多数の部品の空間実装効率を向上させることが可能となっている。三次元CADでは形状の曖昧(あいまい)性を許容しないため、トップダウン設計の導入による仕様決定の上流化が必要である。しかし、性能検証を伴わないデジタル作図(Electronic Product Definition)はあくまで“ハリボテ”であり、背後の物理現象の成立性を検証する手法の充実が同時に必要である。設計上流での物理特性の成立性に対する目利き力の不足から、システム配分を誤ると大きな手戻りが発生して、短期化する開発競争において致命的となる。そこで筆者らは、デジタル設計技術を導入したフロントローディング型実装設計を提案する。この手法では、“Step

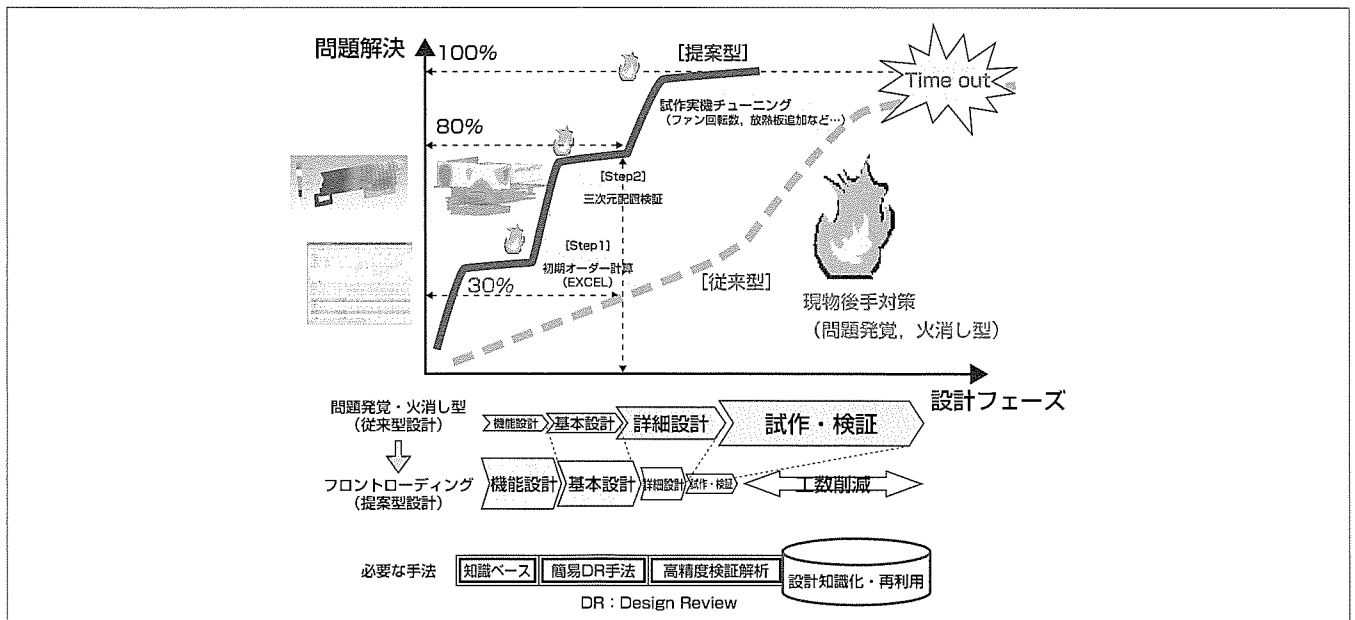
1”と“Step 2”の2段階での実装設計高度化を行う段階的詳細化(Stepwise refinement)を行い、開発フェーズに応じた設計対策案を段階的に盛り込むことで、製品開発のQCD(Quality, Cost, Delivery)の全体改善が実現できる。

- (1) Step 1 : 原理・原則ルールベースに基づいた方式検討
- (2) Step 2 : 詳細条件での三次元解析, 高精度な設計検証

高密度実装機器では三次元的な通風・放熱設計, 構造強度, 振動, 電磁波対策(伝送線路, EMI)などが問題化するため、製品開発のQCDの全体改善を達成するには、設計自由度が高い上流レビューによる配置構造トレードオフ最適化, 相互調整が不可欠である。

本稿では、1DIN型HDDカーナビ機種種の熱, EMI(ElectroMagnetic Interference)の上流設計において上述したフロントローディング型実装設計法を適用し、ファンレス化密閉筐体(きょうたい)を実現したのでこれについて述べる。

特集 II



デジタル設計手法を導入したフロントローディング型実装設計の概念

デジタル設計技術を導入したフロントローディング型実装設計法では、Step 1とStep 2の2段階での実装設計高度化を行う段階的詳細化を行い、開発フェーズに応じた設計対策案を段階的に盛り込むことで、製品開発のQCDの全体改善が実現できる。

1. ま え が き

デジタル技術やネットワーク技術を融合した携帯情報機器、カーナビゲーションシステム、情報家電などは、日本が世界をリードする製品分野として期待されている。これらの分野では、多機能化や高性能化により製品競争力を高めるために、システム規模の拡大と動作周波数の高速化が進んでいる。また、日本のお家芸である機器の小型化(高密度実装)に対する要求も強い。製品アーキテクチャには、大きく分けて2種類がある⁽¹⁾(表1)。

デスクトップ型パソコンに代表されるデジタル機器では、モジュール化された機能ブロック(CPU(Central Processing Unit)、メモリ、HDD(Hard Disk Drive)、標準OS(Operating System)...)を組み合わせることで簡単にシステムの機能設計ができる特長がある。しかし、デジタル面の機能設計が容易化した反面で、機器の高速・高性能化に伴う実装設計面でのアナログ問題(伝送ノイズ、EMI、発熱、振動...)が顕在化している。こうした問題が実機試作段階で顕在化すると、基本設計にまで及ぶ手戻りが発生し、開発期間・対策費用の致命的な増大を招く。つまり、高速・高性能機器での高密度実装設計はインタフェース技術ではなく、付加価値の源泉である統合技術ととらえるべき⁽²⁾であり、前述の“組み合わせ型”と“擦り合わせ型”の各特長を融合した柔軟な設計方法論が必要である。

本稿では、三次元CADやCAE(Computer Aided Engineering)などのデジタルベースの設計手法を開発上流段階から駆使して設計自由度の高い設計上流段階で適切な仕様を作り込むフロントローディング型実装設計手法について述べる。また、同手法をカーナビシステムの開発に適用して短期に高品質な製品を開発した事例についても述べる。

2. フロントローディング型実装設計

近年、三次元CADの干渉チェック機能を駆使して高精度な公差設計により多数の部品の空間実装効率を向上させることが可能となっている。三次元CADでは形状の曖昧性を許容しないため、トップダウン設計の導入による仕様決定の上流化が必要である。しかし、性能検証を伴わないデジタル作図はあくまでハリボテであり、背後の物理現象の成立性を検証する手法の充実が必要である。設計上流での物理特性の成立性に対する目利き力の不足から、システム配分を誤ると大きな手戻りが発生して、短期化する開発競争において致命的となる。筆者らの提案するデジタル設計手法を導入したフロントローディング型実装設計の概念⁽³⁾を図1に示す。特にStep 1と

Step 2の2段階での実装設計高度化を行う段階的詳細化手法を提案している。

- (1) Step 1：原理・原則ルールベースに基づいた方式検討
- (2) Step 2：詳細条件での三次元解析、高精度な設計検証

高密度実装機器では通風・放熱設計、構造強度、振動、電磁波対策構造の三次元的な最適化が必要であり、設計自由度が高い上流段階での三次元配置トレードオフ設計が必要である。

3. 車載カーナビへの適用

今回開発した“1DIN HDDカーナビ”(図2)では、小型筐体((W)180mm×(D)195.5mm×(H)50mm)に高速CPUと高性能グラフィックスエンジンを1チップ化したカーナビ専用ASIC(Application Specific Integrated Circuit)“ナビコア”と、大容量HDDを組み合わせている。その結果、スピーディなスクロール描画、多彩な地図表示の高速処理が可能である(従来比で約8倍の描画性能を実現)。

この機種の熱、伝送・EMIの上流設計において上述したフロントローディング型実装設計を適用し、放熱性とEMI性能を両立したファンレス化密閉筐体を実現したので述べる。

3.1 カーナビの熱設計

カーナビ筐体の設置環境は、エンジンルームや暖房吹出

表1. 製品アーキテクチャ

●擦り合わせ(integral)型	部品設計を相互調整し、製品ごとに最適設計しないと製品全体の性能が出ないタイプ(自動車機器など)
●組み合わせ(modular)型	部品・モジュールのインタフェースが標準化されており、既存部品を組み合わせれば多様な製品が実現できるタイプ。(パソコンに代表されるデジタル機器)

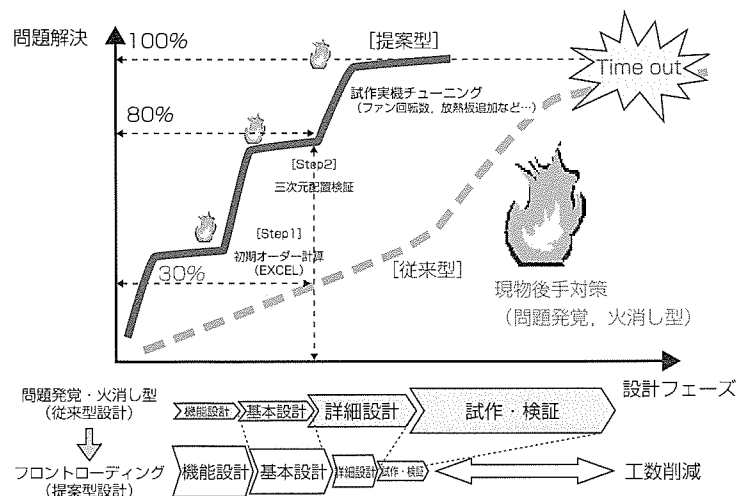


図1. フロントローディング型実装設計のねらい

しに近い場合、一般電子機器よりも20~30℃ほど厳しい熱環境にある。また、車内居住空間のダッシュボード等に実装されるためにファン低騒音化の要求が大きく、ファン風量を抑制せざるを得ない課題がある。

3.1.1 Step 1：原理・原則ルールベースに基づいた冷却方式検討

基本設計段階に必要な情報は、“○；設計継続可(白)”，“×；設計見直し(黒)”，“△；要注意(グレー)”の大きな実現目処を製品成立性に関して把握することである(First Order Estimation)。設計上流の検討では不確定な設計要素が多いため、解析精度よりも試行錯誤を短期間に繰り返せる迅速性が重要であり、表計算シートを用いた簡易計算ツール(Spread sheet Aided Engineering：SAE)も整備している。図3はカーナビ筐体内部の平均空気温度を予測可能な簡易設計式を用いた簡易解析(First Order Analysis)ツールであり、ファンの必要有無や必要換気風量を上流段階で検討できる。実測との差異は20%と許容範囲内であり、上流DR(Design Review)には十分な高速性、精度を持っている。

3.1.2 Step 2：詳細条件での三次元熱流体解析

筐体内のデバイスレイアウトを検討する段階では、三次元熱流体解析を駆使して詳細な温度分布を予測・検証する(図4)。今回の機種では、以下(1)~(3)の対策アイデアをシミュレーション検討することで、筐体の保有する放熱性能を最大限に引き出したファンレス化密閉筐体を実現した。



図2. 1DIN型HDDカーナビ

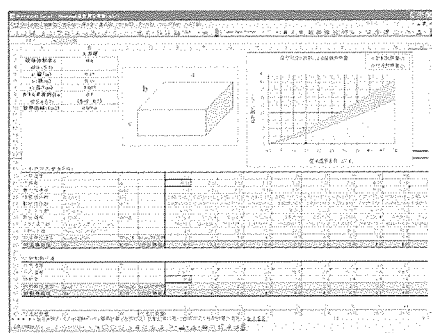


図3. 表計算シートを用いた簡易熱計算ツール

- (1) CPU発熱のAI放熱板への拡散
- (2) 筐体内デバイス、基板上的最適部品配置と温度最適化
- (3) DVD(Digital Versatile Disk), HDD用板金の利用による放熱効率向上

試作筐体での熱評価では対策レスで温度条件をクリアでき、工程どおりに出荷を開始した。この手法の適用により、ファンレス化によるコスト原低、耐塵埃(じんあい)性の向上、低騒音化(従来ファン筐体30dB(A)→今回、ファンレス筐体25dB(A))などの製品実装品質の向上を実現した(図5)。

3.2 カーナビの伝送線路・EMI設計

車載機器ではCPUとメモリ間の動作周波数が100MHzと高速化して信号伝送設計が難しくなっており、EMI規制のクリアレベルもより厳しくなっている。また、高密度実装が進む中、筐体や基板が持つ形状固有の周波数特性と回路の動作周波数が共振し、高調波が重なる放射ノイズが発生する課題もある。

3.2.1 Step 1：原理・原則ルールベースに基づいた伝送・EMI方式検討

基本設計段階では、ダンピング抵抗やパスコンの位置、

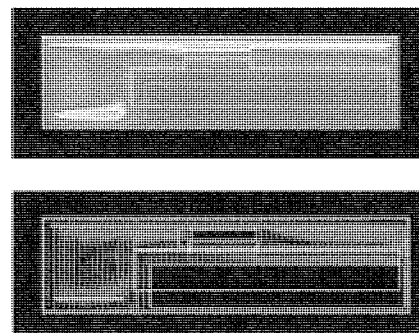


図4. 詳細レイアウト条件での三次元熱流体解析

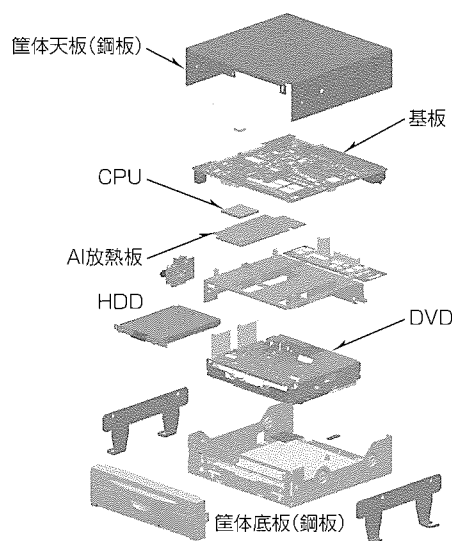


図5. HDDカーナビの三次元レイアウト

配線設計、フィルタの要否などをルールベースに基づき初期検討する。当社では、伝送・EMI設計に関する原理・原則をまとめた設計データベースを社内イントラネット上でポータル画面として設計者へ提供し、実装設計情報の共有化を図っている⁽⁴⁾。このレビューシステムでは膨大なチェック内容から各設計ステップに必要なチェック項目を抽出してチェックでき、その根拠となる文書、データにハイパーリンクで瞬時にアクセスし参照できる。

3.2.2 Step 2：詳細条件での伝送線路解析と三次元EMI共振解析

(1) 伝送線路解析

配線段階ではCLK (CLocK) 信号等の重要な信号に対して伝送線路解析による波形検証を行い、最適な配線の引き直しや配線層、部品配置を決定する(図6)。また、素子の駆動能力に合わせてダンピング抵抗の定数や要否を決定し、基板設計に反映する。

(2) 三次元EMI共振解析⁽⁵⁾

構想レイアウト段階では、共振が発生する周波数帯を予測し、問題となる周波数での共振を回避する設計を行う。一例として、共振周波数が異なる筐体の開口部や、基板形状、ネジ止め位置、GND (GrouND) 接続の実装形状の影響を三次元概略形状モデルでEMI共振解析を行った結果を図7に示す。この解析により、試作測定では困難な何パターンもの実装構造のトレードオフ検討、最適化が上流設計段階で可能となる。

4. む す び

以上、設計ルールベース、簡易設計式や三次元簡易解析手法を段階的に適用して設計上流に効果的に実装設計品質を作り込むフロントローディング型設計手法につき述べ、カーナビ製品への適用事例からその有効性を示した。

近年のIT革命に伴い、設計現場の設計環境・開発スタイルが激変している。実装設計分野においても、簡易計算ツールや三次元CAEを始めとしたデジタル設計体系の使い分け戦略、全体プロセス最適化ビジョンを再構築し、創造的に価値創生(Quality)、コストダウン(Cost)、納期短縮(Delivery)を達成していく必要がある⁽⁶⁾。

参考文献

- (1) 藤本隆宏, 日本のもの造り哲学, 日本経済新聞社刊 (2004-6)
- (2) 貫井 孝: 電子システムインテグレーションと新「実装技術(者)」像, エレクトロニクス実装学会誌, 5, No.7, 巻頭言 (2002-11)

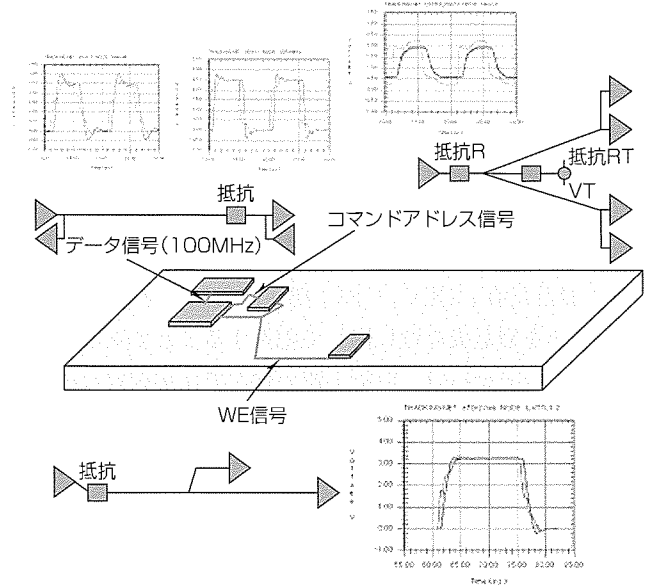


図6. 伝送線路解析

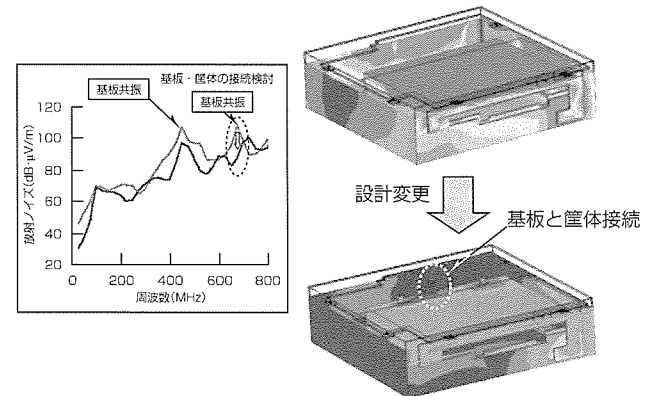


図7. EMI共振解析

- (3) 小林 孝, ほか: 上流設計の重要性とその手法, 日本機械学会 第13回設計工学部門講演会 公開討論原稿, 174~176 (2003-10)
- (4) 小林 孝, ほか: デジタル機器における実装設計フロントローディング手法(携帯型IP電話やノートパソコン開発への適用), 日本機械学会2004年度年次大会, (2004-9)
- (5) 堀越美香, ほか: CAE解析による小型情報機器の筐体・基板のEMI設計, 第19回エレクトロニクス実装学会学術講演大会 講演論文集, 41~42 (2005-3)
- (6) 小林 孝: 電機製品開発における最適設計の必要性とその適用事例, 日本機械学会誌(小特集: 最適設計のフロンティア), 62~64 (2006-5)

衛星開発における設計／製造品質の向上と効率化

川口浩知* 石井芳征**
 佐藤 博**
 戸塚正弘**

Improvement of Quality and Efficiency in Satellite Development

Hirochika Kawaguchi, Hiroshi Sato, Masahiro Tozuka, Yoshiyuki Ishii

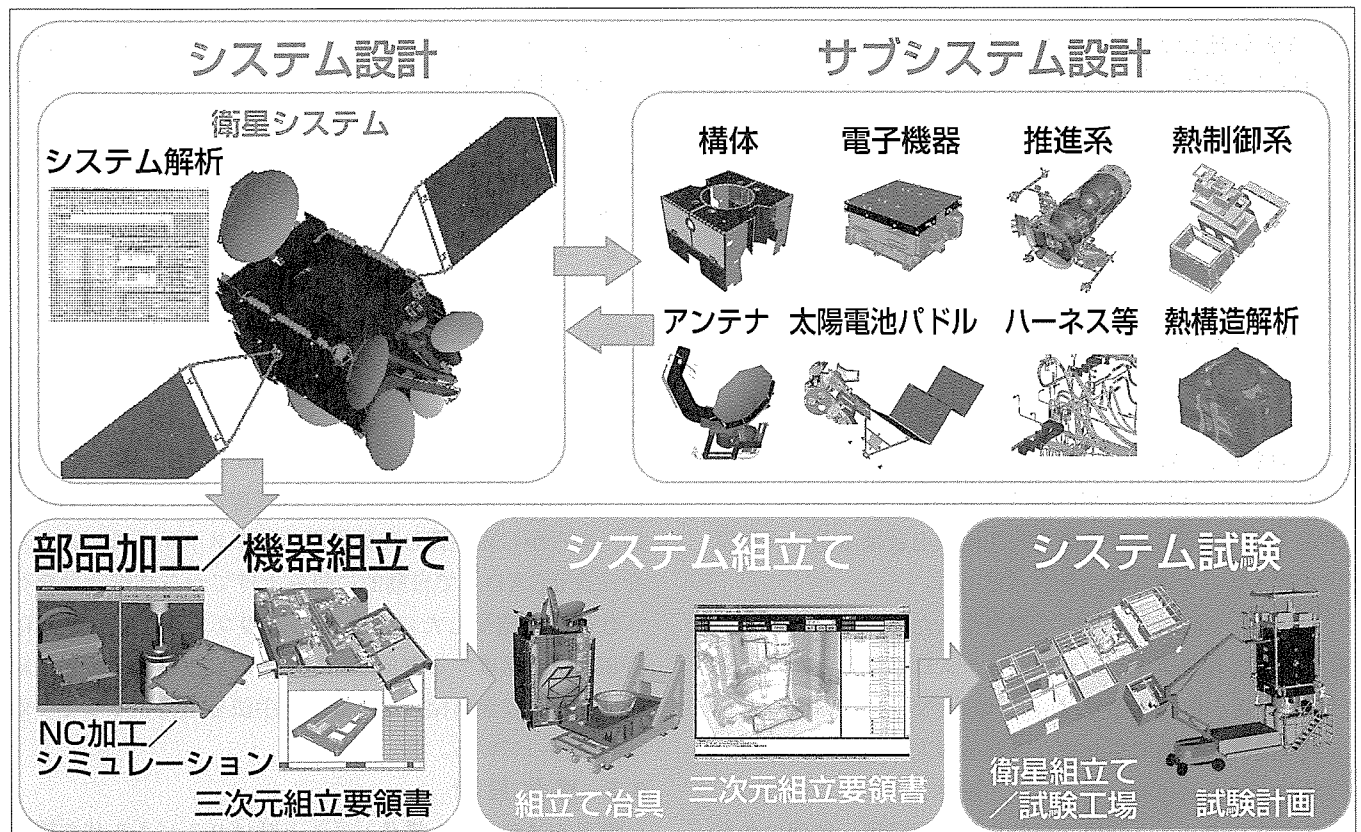
要 旨

国際入札による商用衛星を受注するには、三菱電機がこれまでの衛星開発で蓄積してきた高品質・高信頼性技術を更に向上させつつ、欧米メーカーに比肩する短納期・低コストへの更なる追求が不可欠である。

当社では、宇宙標準化活動として、調達から設計・製造・試験・運用に至るすべてのプロセスにおける技術の標準化とプロセスの標準化を行い、さらに、すべてのプロセスの生産性向上を目的に、IT技術を活用した設計生産革新に取り組んでいる。

設計生産革新活動は、客先提案から調達・設計・製造・試験・運用、さらには経営・生産管理など、業務全体の品質向上及び効率化を目的としている。

本稿では、その中でも、三次元設計生産を中心とした衛星の設計生産革新の取り組みについて述べる。また、商用衛星の受注と生産効率化を目標に取り組んできた標準化・効率化の成果を当社標準衛星シリーズの静止通信衛星に適宜適用することで、客先提案設計及び衛星開発の早期立ち上げを実現している状況について述べる。



三次元データを核とした人工衛星の設計生産革新

短納期・低コスト・高品質な衛星開発プロセスを実現するため、三次元設計データを核とした設計生産革新に取り組んでいる。部品点数が多く技術分野が多岐にわたる衛星開発では、設計データを設計部門間で確実かつ効率的に運用しながら設計することが重要である。また、製造・組立て・試験の各工程で、製造装置とのデータ連携や、人手作業を三次元データによりナビゲートする仕組み作りが重要となる。

1. ま え が き

将来の高度な宇宙利用技術や宇宙／地球環境の研究，新たな人工衛星の技術開発を目的とした研究開発型の人工衛星に対し，通信／放送など我々の生活に密着した社会システムの一部としての人工衛星(商用衛星)は，欧米の衛星システムメーカーとの競争を経て受注される。

このような商用衛星市場での国際競争力を確保するには，これまでの研究開発型の衛星開発で積み上げてきた高品質・高信頼性技術に加え，欧米の衛星システムメーカーに比肩する短納期・低コストの実現が重要となる。

衛星システムを設計／製造している当社鎌倉製作所では，これまでに開発してきた人工衛星を基盤に更なる技術の高度化を図るとともに，宇宙標準化活動として，標準プラットフォームの開発や，調達から設計・製造・試験・運用に至るすべてのプロセスにかかわる技術の標準化とプロセスの標準化を行っている。また，すべてのプロセスの生産性向上を目的に，IT技術を活用した継続的な設計生産革新に取り組んでいる。

2. 衛星設計生産革新の取り組み

鎌倉製作所では，宇宙，防衛，通信システム等の各基幹事業における調達・設計・製造・試験・運用，さらには経営・生産管理など，業務全体の品質向上及び効率化を図っている。本稿では，その中でも，三次元設計生産を中心とした衛星の設計生産革新の取り組みについて述べる。

衛星システムは，ハードウェアの保守ができない宇宙環境下で10年以上もの動作保証が要求されるとともに，打ち上げ時の振動や衝撃，運用中の温度環境・放射線環境が地上よりもはるかに厳しい。このため，耐環境構造や環境から受ける影響を制御する構造，さらには冗長系を多数採用して信頼性を確保するなど，複雑なシステムとなっている。また，通信システムを介した地上管制センターからの監視・遠隔操作に加え，自己や周囲の状況をモニタしながら制御するなど自律性の高い製品でもあり，部品点数にしてロケットの2倍以上，自動車の70倍以上とはるかに大規模かつ複雑なシステム製品となっている。

このような衛星システムを開発するための技術分野及び衛星システムを構成するサブシステムは多岐にわたる。設計生産革新の取り組みでは，これらサブシステム設計とシステム設計との間でやり取りされる膨大な量の設計情報を確実かつ効率的に運用することが重要となる。このため，設計作業やチェック作業の自動化，履歴管理，情報の共有化／見える化が，効率化だけでなく，後工程からの手戻りを防止する上でも重要となる。

3. 三次元設計による品質／効率向上

三次元CAD(Pro/ENGINEER^(注1))を活用した衛星設計の効率化に取り組む中で，独自に開発してきた特徴的な三次元設計手法と，その活用事例について述べる。

3.1 システム設計

システム設計では，客先要求に従って各サブシステム設計と調整を行いながら衛星システム全体の取りまとめ，サイジング／レイアウト検討を行っている。

全体を取りまとめるシステム設計では，大規模な三次元データを複数のサブシステム設計と協調／連携し，確実かつ効率的に運用しながら設計を進めていくことが重要となる。一般的に三次元CAD(Computer Aided Design)を用いた設計では，常に最新の設計データを設計部門間で共有しながら設計を進めていく手法が利点として挙げられているが，衛星システムのような大規模設計では，必ずしも有効な手段とはならない。各設計部門の日々の検討過程を互いに共有することは小さな手戻りを許容することであるが，大規模設計ではこの影響が広く波及するため，設計の収束を遅らせる原因となってしまう。そこで，三次元データを設計部門間で共有しながらも，検討過程のデータは互いに共有せず，部門が承認した設計データのみを共有する設計手法を採用している。具体的には，サブシステム設計部門で設計データが承認された時点で，システム設計部門に必要な設計情報(形状情報や取り付け点，コネクタ等の情報)を取捨選択してコピーモデル(Interface Control Model: ICM)に反映し，システム設計や他のサブシステム設計で利用している。

3.2 コンポーネント設計

衛星システムに搭載される電子機器(コンポーネント)の設計では，基板CADの情報等を利用しながら筐体(きょうたい)設計やCAE(Computer Aided Engineering)による熱／構造解析，放射線解析等の事前検証を行っている。基本的に三次元CADの一般的な使用方法で設計を進めるが，標準化が進んでいるスライス構造のコンポーネントでは，あらかじめ整備した数種類の標準スライスモジュールを三次元CAD上で自動的に組み上げてから詳細設計を行う仕組みを開発したほか，通信系のコンポーネントでは，接続システムを構成する電子部品の効率的な配置手法や，接続システムの形状に金属筐体を彫り込む手法を開発することで効率化を図っている。

3.3 構体設計

衛星システムは，構体パネルと呼ばれるパネル状の構造部材を箱状に組み合わせ，その両面にコンポーネント等

(注1) Pro/ENGINEER, Pro/SHEETMETAL, Pro/PIPING, Pro/CABLINGは，米国Parametric Technology Corp.の登録商標である。

を固定して構成されている。構体パネル内部にはヒートパイプが埋め込まれ、パネルそのものは軽量かつ高剛性なアルミハニカム構造材／カーボン複合材で構成されている。構体設計では、設計標準化による三次元雛形(ひながた)データを基にCAE構造解析までを行うが、特にクリティカルな工程として、システム設計部門がレイアウトするすべてのコンポーネント締結点の位置情報を確実に構体設計／製造に反映する工程がある。この締結点は数千点に及び、構体パネルにNC(Numerical Control)で穴開け加工する際、内部に埋め込まれたヒートパイプと干渉しないよう、システム設計のレイアウト検討段階で、ノミナル寸法に製造／組立て公差を考慮した干渉チェックを行い、構体設計及び製造からの手戻りをなくしている(図1)。

3.4 熱制御系設計

衛星は、太陽との位置関係が常に変化することから、 $-200\sim+150^{\circ}\text{C}$ の温度サイクルに常にさらされている。このため、衛星は、放熱面だけでなく、低温化を防ぐヒーターや、衛星全体に熱を伝導させるヒートパイプ、及び熱入力を抑制する多層断熱材(Multi Layer Insulation: MLI)で熱を制御している。MLIはシート状の断熱材であり、衛星表面の凹凸を覆うようペーパークラフト細工のように折り曲げて組み立てられる。衛星表面にはこれが数百枚取り付けられており、設計では、MLIの仕上がり形状が衛星にフィットするとともに、衛星とMLI、MLI同士の取付け点の間違いなく整合することが重要となる。設計部門では、三次元板金CAD(Pro/SHEET METAL^(註1))を活用して、MLIを衛星に装着した状態で設計し、これを自動展開して展開図面を作成している。また、MLI上の取付け点の位置・形状・タイプを、MLI間／衛星間で共有しながら展開する手法を開発し、取付けにおいても不整合のない設計を実現している(図2)。

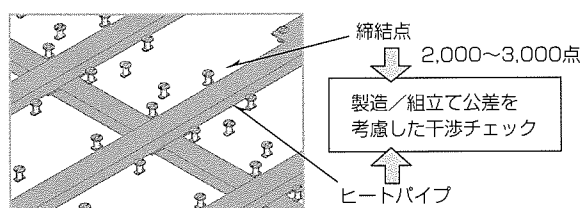


図1. 締結点とヒートパイプの干渉チェック

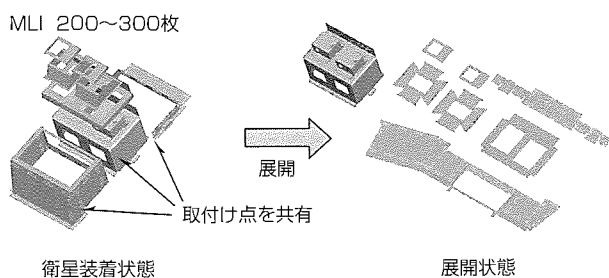


図2. 取付け点を共有しながら展開するMLI

3.5 推進系設計

衛星システムには、衛星の軌道及び姿勢を制御するための噴射ノズル(スラスター)が複数配置され、推進剤の入ったタンクとの間を制御装置や百本以上の配管で接続されている。推進系配管の設計では三次元配管CAD(Pro/PIPING^(註1))を利用して配管の長さ計測を自動化するとともに、図面上に記載する曲げ点座標表の自動作成や、曲げ点座標データを曲げ加工機に入力する仕組みを開発するなど、効率化と品質向上を図っている(図3)。

3.6 同軸ケーブル設計

コンポーネント間を接続する数百本に及ぶセミリジッド同軸ケーブルでも、推進系配管の設計同様、三次元配管CAD(Pro/PIPING)を利用して、線長の把握(フレキシブル同軸ケーブルも同様)、図面情報、曲げ加工データの作成を自動化し、効率化と品質向上を図っている(図3)。

3.7 導波管設計

一般的な静止通信衛星の場合、千本以上もの導波管でコンポーネント間が接続されている。導波管は長方形断面で、断面が捩(ねじ)れたツイスト導波管や断面サイズが両端で異なるテーパ導波管などがある。導波管の設計では、三次元配管CAD(Pro/PIPING)を活用し、ルート検討作業や、製造単位に導波管を分割する作業、導波管の接合フランジやコーナーピースの配置作業を効率化している。図面作成においては、類似形状の導波管を自動分類して図面を自動作成する仕組みを開発し、設計／製造の効率化と品質向上を図っている(図3)。

3.8 ハーネス設計

コンポーネント間を接続する1万本を超えるワイヤハーネスは、1本1本を人手によりコネクタピンへ挿入し、引き回しが行われており、その束径は太い箇所では40~50mmに及ぶ。このことから、平展開したハーネスを後から曲げて組み付けることができず、ハーネスボードと呼ばれる衛星を模擬したダミーボード上で製作する。また、衛星の配線経路は立体的で複雑であり、コネクタの数も数百~千個程度と多く、組立て作業者が配線経路やコネクタの位置を特定する作業も容易ではない。そこで、組立て現場で三次

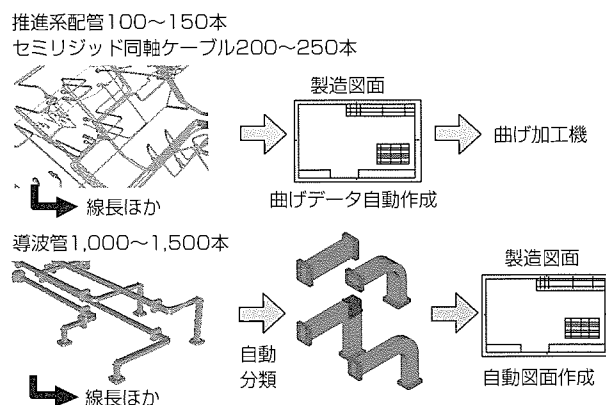


図3. 推進系配管, 同軸ケーブル, 導波管の設計/製造

元データを活用し、配線経路とコネクタ位置をナビゲートする仕組みを開発し、組立て作業の効率と品質を向上している。配線経路をナビゲートするには、接続情報を持った三次元データが必要なため、設計部門では、コネクタピン間の接続情報(ワイヤリスト)を三次元配線CAD(Pro/CABLING^(註1))に取り込み、あらかじめ配置した通過点上にハーネス形状を自動作成している。設計では、この三次元データを、電気設計と機械設計の整合性確認や、ハーネスの束径/線長/重心/慣性モーメント等の自動計算に利用している。そのほか、東部の配線構成を三次元データから自動抽出し、発熱量の迅速な見積りに役立っている(図4)。

3.9 太陽電池パドル設計

太陽電池パドルは、大型の通信アンテナ同様、ロケットによる打ち上げ時には閉じており、軌道上で展開して使用される。設計では、数学モデルを用いた動的なCAE機構解析を行うとともに、展開の過程で機構部品に干渉が生じないように、別途三次元CAD上で詳細部品を動作させてチェックする必要がある。三次元CADの一般的な特徴を利用して、太陽電池パドル全体の展開状態と各機構部品の展開状態を同期する仕組みにすると、個別に各機構部品の展開状態を検討した結果が太陽電池パドル全体に反映され、衛星システム全体の状態にまで影響を及ぼしてしまう。そこで、全体の動作を連動させつつも、個々の動作を独立して検討できるような設計手法を開発し、利便性と品質の向上を図っている。

4. 製造/試験での三次元設計データ活用

部品加工に三次元データを用いNC加工等を行うことは製造業で一般的であるが、鎌倉製作所では、人手による作業が主体である組立て作業においても三次元データを有効に活用している。例えば、三次元ビューワデータと三次元データ以外の設計データを連携させてシステム化し、ディスプレイ画面を見ながら組立て作業をナビゲートしている。利便性から併用する紙の図面も三次元データに持たせた製造情報は記載しないなど、合理化も同時に進めている。

そのほか、衛星の組立て/試験に関するレイアウト検討に、工場全体及び組立て/試験設備の三次元データを活用するなど、三次元ビューワの導入により、ほぼすべての部門で三次元データの利用が進んでおり、関係者のレビューや設計意図の伝達が正確になり、手戻り抑制や品質向上に役立っている。

5. 衛星商用化に対応した更なる効率化

商用衛星では、高品質・高信頼性を維持向上させながら、更なる短納期・低コストの実現が重要となる。当社では、当社標準衛星シリーズに対し、これまでに開発・実践してきた設計手法や設計システムだけでなく、商用衛星の受注

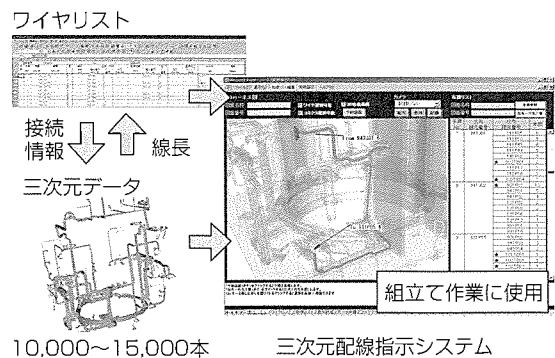


図4. 三次元データを活用したハーネス組立て

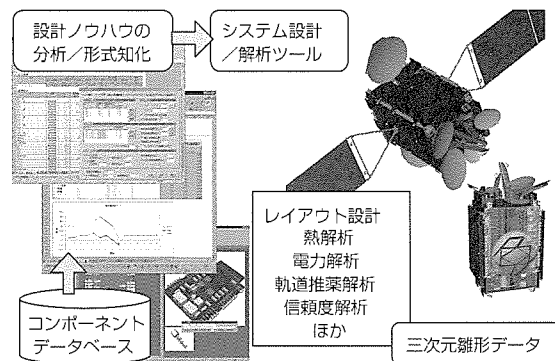


図5. 商用衛星における標準化・効率化の取り組み

と生産効率化を目標に取り組んできた成果の活用も行っている。例えば、各分野の設計者の持つ設計ノウハウを分析して形式知化し、パラメータやプロセスの標準化を行いツール化した。その結果、客先提案までの期間を欧米水準にまで短縮しながらも、当社が蓄積/向上してきた衛星開発技術により、高い技術提案を現実のものとしている。また、これまでに整備してきた衛星の三次元雛形データやデータベースを活用し、設計の早期立ち上げを実現している(図5)。

6. むすび

本稿では当社の衛星開発における設計/製造の効率化と品質向上の取り組みについて述べたが、衛星の開発プロセスは、製品規模に相応して大規模であり、詳細に全容を把握することは非常に困難である。このため、開発プロセス全体の統合的な効率化にはまだ至っていないが、特に商用衛星では短納期化が顧客満足、国際競争力の維持向上に不可欠であり、今後も当社標準衛星シリーズの開発プロセスを継続的に分析し、更なる短納期化を進めていく。

参考文献

- (1) 佐藤 博, ほか: 衛星開発デジタルイノベーション, 三菱電機技報, 75, No.2, 124~127 (2001)
- (2) 山形史郎: 大型宇宙システムを支える最新のシステム開発マネジメント技術, 日本航空宇宙学会誌, 50, 283~290 (2002)

車両用モータの熱設計フロントローディング

羽下誠司*
坂根正道**

Front-Loading of Thermal Design for Motor of Railroad Car

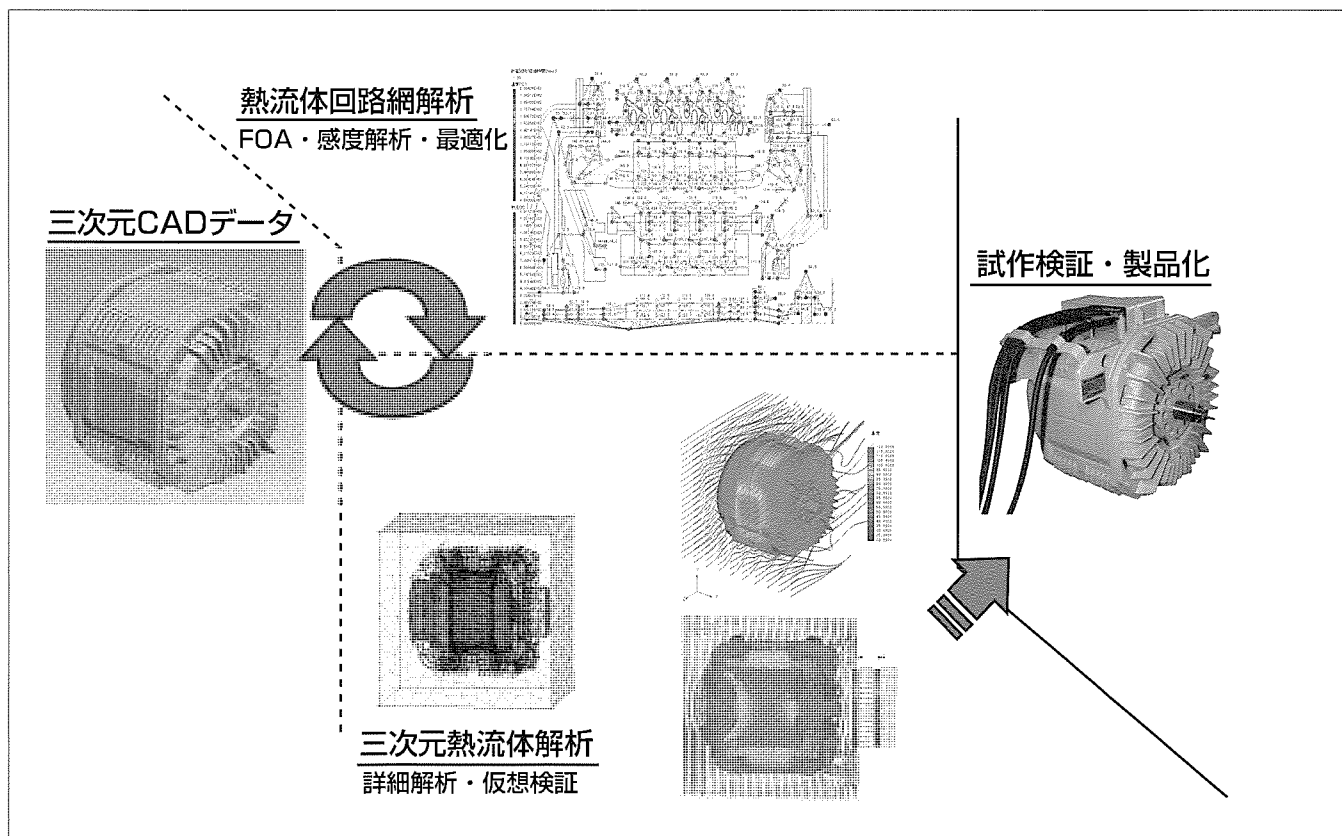
Seiji Haga, Masamichi Sakane

要旨

車両用モータでは、限られた取付けスペースの中で小型軽量化・大容量化が求められており、通常、高い温度で使われる。その一方で、軸受の潤滑にはグリースを使用しているが、グリースの潤滑性能を長期的に維持するには、温度は常温に近いほど良い。車両用モータの開発段階では、コイル・回転子パー温度は許容範囲内にあるが、軸受温度がグリース耐熱温度の許容範囲をオーバーするという状況がしばしば発生し、試作・試験後の冷却構造の見直し・改造などが設計手戻りの要因の一つとなっている。そこで、試作前での温度上昇予測精度向上のための高精度熱流体解析技術を開発し、熱設計のフロントローディング化を実現した。

一方、最近の鉄道車両用駆動システムには、車両の高速化に伴う高出力化・小型軽量化とともに、省保守化の追求及び車内外騒音の低減などに対応して、モータ(主電動機)の全閉化が要求されている。鉄道車両用の全閉形主電動機としては、三菱電機が国内初の商品化を達成している。

このような全閉形主電動機の開発では、従来の開放形主電動機より冷却が大幅に困難になるため、冷却構造を抜本的に見直す必要があった。冷却構造の検討に当たっては、熱回路網法により様々な冷却方式の検討を実施し、基本構造を決定した。さらに、駆動側軸受を効率良く冷却する必要があったため、三次元熱流体解析を用いてその冷却構造設計を実施し、温度目標値をクリアした。



車両用モータの熱流体解析技術

車両用モータは、車両の高速化に伴う高出力化・小型軽量化が求められているが、さらに、省保守化の追求及び車内外騒音の低減などに対応して、モータの全閉化が要求されている。モータの全閉化により冷却構造が複雑化し、従来の試作・試験主体の開発スタイルでは熱流動現象の把握及び適切な対策案の立案が困難になってきている。そこで、車両用モータの開発・設計段階において適用可能な熱流体解析技術の開発を実施した。外扇付き全閉形主電動機の開発に適用し、全閉形主電動機としては国内初の商品化に貢献している。

1. ま え が き

車両用モータでは、限られた取付けスペースの中で小型軽量化・大容量化が求められており、通常、高い温度で使われることになる。その一方で、軸受の潤滑にはグリースを使用しているが、グリースの耐熱温度は鉄心等に比べれば低く、長期的に潤滑性能を維持するには温度は常温に近いほど良い。そのため、高温で使われるモータにあって、いかに軸受温度を低く保つ設計をするかが長期信頼性設計において重要な要素であり、車両用モータにおける熱設計フロントローディングのキーポイントである。

2. 車両用モータにおける熱設計の課題

車両用モータの開発段階では、鉄心部のコイル・回転子バー温度は許容範囲内にあるが、軸受温度がグリース耐熱温度の許容範囲をオーバーするという状況がしばしば発生し、試作・試験後の冷却構造の見直し・改造などが設計手戻りの要因の一つとなっている。特に近年、徐々に冷却構造が複雑化する状況において、試験のみでは熱流動現象の把握が非常に困難になり、試作・試験を主体とした対策案検証作業は困難になりつつある(有効な対策案がなかなか得られず、試作・試験回数が増大してしまう)。その課題の有効な解決手段は、熱流体解析(シミュレーション)による温度上昇値予測及び電磁界解析技術による損失(発熱量)予測技術の高度化である。

試作前に解析でモータが発生する発熱量及び軸受温度を把握し事前に対策することができれば、試作・試験段階の不具合・手戻り発生を未然に抑制し、早期製品化が可能となる(フロントローディングの実現)。これを実現するには、設計変更前後の発熱量及び温度上昇値の定性的な傾向、又はその絶対値をいかに精度良くとらえるかが重要となる。さらに、複雑な風路とファン形状の組合せにより定まる冷却風の風速・風量においても事前に精度良く予測することが重要である。しかし、車両用モータでは、限界まで冷却性能を高めるために設けられた特殊な風路構造及び自己冷却ファン、さらに、モータ自身の大きさ(計算格子数の増大)により、熱流体解析を困難にしていた。

そこで、複雑なモータの熱設計を効率的に実施する方法として、車両用モータに適した以下の2段階の熱流体解析技術を開発した。

(1) 第1段階：熱流体回路網法⁽¹⁾によるオーダー解析

熱流体回路網法は、熱流動現象を電気回路のような等価回路に置換してモデル化する手法であり、計算点数が百数十点と少なく、計算時間が非常に短い(数秒)という特長がある。そのため、短時間に多くの解析が実行できるため、FOA(First Order Analysis)やフィージビリティスタディ(感度解析・最適化)に向く手法である。ただし、熱流体回

路網構築には専門的な知識・経験(実測値との合わせ込み等)が必要となる。

(2) 第2段階：三次元熱流体解析による詳細解析

製品形状に基づき詳細に解析する手法である。熱回路網法より高精度な解が得られるが、その反面、計算時間は増大する。三次元熱流体解析は、試験の置き換えや、さらには試験では得られない様々な知見(冷却風の流れの可視化、詳細な温度分布等)を得ることができるため、試作前の最終的な熱設計の妥当性の評価、又は回路網法ではモデル化しきれない設計変更の影響などの評価に使うことができる。三次元解析用計算格子(メッシュ)作成の課題に対しては、三次元CAD(Computer Aided Design)データの利用と自動メッシュ生成機能で効率化を図った。

3. 車両用モータ熱解析技術

3.1 車両用モータの熱流体回路網モデル

3.1.1 熱流体回路網法の概要

熱流体回路網法は、伝熱現象及び流体の流れを電気回路のような等価回路に置き換える手法である。熱回路網の基礎式を式(1)に、流体回路網の基礎式を式(2)に示す。

$$Q = \frac{\Delta T}{R} \dots\dots\dots(1)$$

Q: 伝熱量(W), ΔT: 温度差(K), R: 熱抵抗(K/W)

$$W = \frac{\Delta H}{Z} \dots\dots\dots(2)$$

W: 質量流量(kg/s), ΔH: 全圧差(Pa), Z: 流体抵抗(1/(m・s))

抵抗間の接続点(節点: ノード)において、熱量Q及び質量流量Wの総和が0となる連立方程式を解くことにより、各ノードの温度、圧力を求めることができる。熱抵抗R及び流体抵抗Zは、伝熱現象や流路形状に応じて決定する必要があるが、その設定には専門的な知識・経験(実測値との合わせ込み等)が必要となる。

3.1.2 車両用モータの熱流体回路網解析事例(図1)

熱流体回路網法の解析ソフトウェアでは、社内で開発し

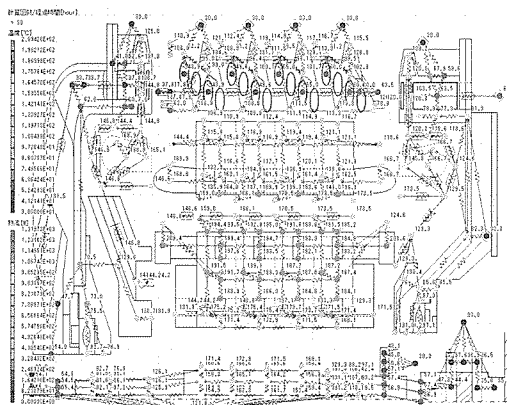


図1. 車両用モータの熱回路網モデルと解析結果表示例

た“TherfBENCH”(サーフベンチ)／“MelTHERFY”(メルサーフィ)を使用している。TherfBENCHは熱流体回路網ソルバMelTHERFYの専用プリポストプロセッサであり、熱流体回路網の部品化・データベース化機能(図2)、設計変数を使用した数式登録機能(例、寸法から熱流長さや放熱面積を計算：図3)、最適化計算機能を持っている。この部品化・設計変数の数式化機能により、車両用モータに特化した熱流体回路網モデルを構築した。これにより、熱回路網部品の交換による冷却構造検討の効率化を実現するとともに、設計変数の感度解析・最適化計算が効率的に実施できるようになり、従来より適切な冷却構造対策案を得ることができるようになった。

3.2 車両用モータの三次元熱流体解析技術

3.2.1 三次元熱流体解析の概要

三次元熱流体解析はCFD(Computational Fluid Dynamics)とも呼ばれ、二次元又は三次元の計算格子(メッシュ)に対し、ナビエ・ストークス方程式及びエネルギー方程式を解くことにより、流体場及び流体・固体内外の伝熱現象を解析する手法である。三次元熱流体解析では、熱流体回路網法のように事前に熱抵抗・流体抵抗を設定する必要は基本的にはなく(計算結果として熱抵抗・流体抵抗が得られる)、メッシュ形状やスキーム(差分手法、計算手順等)

により計算結果が左右される。現在では多数の市販ソフトウェアが流通しているため、用途に応じた適切なソフトウェアの選択と、そのソフトウェアに特化したメッシュ生成のノウハウを構築することが重要である。

3.2.2 車両用モータの三次元熱流体解析事例

(1) 解析用三次元モデルの構築

近年、コンピュータの低コスト化・高性能化及び三次元CAD(三次元設計)の普及により、現在では、三次元CADデータを利用した三次元熱流体解析が一般的になりつつある。すなわち、設計中の三次元CADデータを流用することで、比較的容易に熱流体解析用の三次元CADデータを構築することができる。ただし、三次元設計により実機とほぼ等しい三次元モデルが得られたとしても、現在のコンピュータでは無修正でその三次元データを熱流体解析ソフトウェアに取り込むには、まだまだスペックが不足している。そこで、三次元データの特徴を維持したまま、形状の簡略化を行う必要がある(図4)。

(2) 三次元熱流体解析用メッシュの生成

今回は市販の三次元熱流体解析ソフトウェアを使用しているため、メッシュ生成手法はそのソフトウェア特有の手法であるが、三次元熱流体解析ソフトウェアの選定に当たっては、特に三次元CADデータインタフェース機能、自動メッシュ生成機能のロバスト性、計算速度、計算結果処理(表示)機能が総合的に高いものを選択した。そのため、図4(b)の三次元データを取り込み、そのまま自動メッシュ生成することが可能となり、三次元メッシュ生成作業を大幅に効率化した(図5)。

(3) 計算時間及び計算精度

計算時間はメッシュ数や計算機スペックにもよるが、現

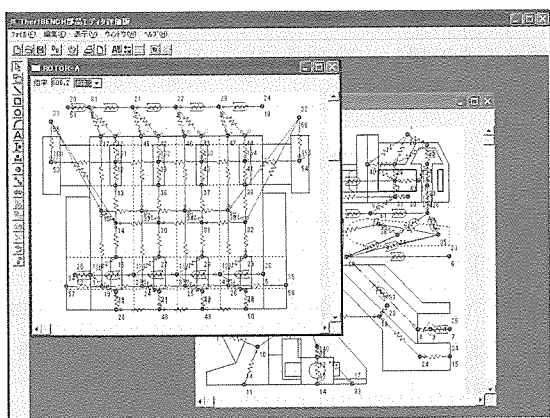


図2. 熱回路網の部品化・データベース化機能

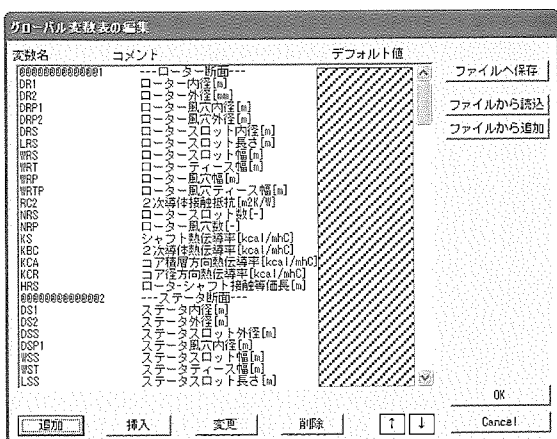
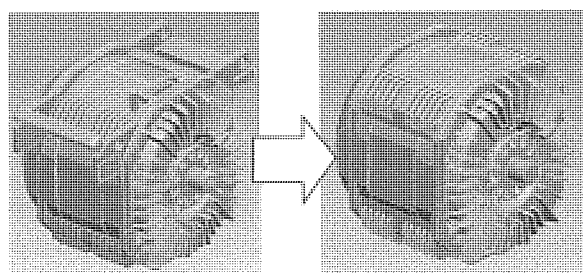


図3. 設計変数一覧



(a) 設計データ(簡略化前) (b) 解析用簡略データ(簡略後)

図4. 三次元モデルの簡略化

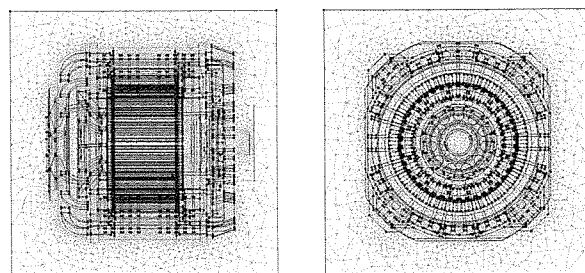


図5. 三次元熱流体解析用の計算格子(メッシュ)

在では平均的に1ケース約6～12時間(1CPU(Central Processing Unit)当たり)程度である。熱流体回路網法に比べれば計算時間はけた違いに増大しているが、この程度の計算負荷であれば、数日中に複数の設計案を比較・評価することが可能であるため、十分に実用的である(CPUの数を増やすことにより、同時に検討できる数を増やすこともできる)。

実測と解析値の誤差(計算精度)に関しては、ファンが発生させる風量では10%以下、温度上昇値でもおおむね10%前後で一致するメッシュ生成手法及び三次元CADデータ簡略化手法を確立した。

なお、解析結果表示例を図6に示す。モータ内部の冷却風及び空気温度分布、モータ全体の詳細な温度分布を可視化できるようになった。

3.3 車両用モータ熱解析技術開発の結論

以上の熱流体回路網法と三次元熱流体解析による2段階の熱設計手法の確立により、試作・試験の前段階で短時間により多くの検討が可能となり、さらに、熱設計に起因する試作・検証作業の多くを解析に置き換えられるようになった。

4. 適用事例

4.1 全閉外扇形主電動機の冷却構造開発

最近の鉄道車両用駆動システムには、車両の高速化に伴う高出力化・小型軽量化が求められているが、さらに、省保守化の追求及び車内外騒音の低減などに対応して、モータ(主電動機)の全閉化が要求されている。このような全閉形主電動機の開発では、従来の開放形主電動機より冷却が大幅に困難になるため、冷却構造を抜本的に見直す必要があった。冷却構造の検討に当たっては、熱回路網法により様々な冷却方式の検討を実施し、基本構造を決定した。一方、長期信頼性確保のため、駆動側軸受を効率良く冷却する必要があったが、そのための冷却対策形状を具体的に三次元熱流体解析を用いて決定することで温度目標値をクリアし、製品化の目処を得た。この全閉外扇形主電動機は、従来の開放形主電動機に対して、モータ単体では6dB

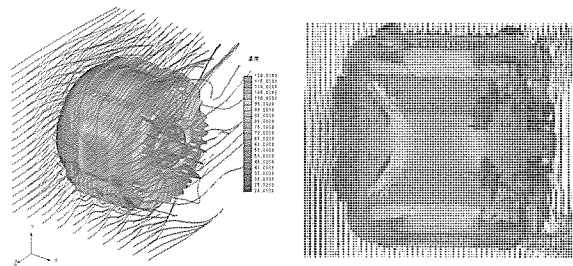


図6. 車両用モータの三次元熱流体解析結果表示例

(A)の低騒音化を達成し、国内初の商品化を実現している(1時間定格:135kW, 1,130V, 95A)。

4.2 他製品への展開

これら熱設計フロントローディング技術は、従来の開放形主電動機(通勤・近郊形車, 新幹線向け)、全閉形主電動機の大容量化, 新方式モータの開発や他製品の開発にも展開中である。

5. むすび

熱流体回路網法及び三次元熱流体解析技術の確立により、車両用モータの熱設計におけるフロントローディングに取り組み、低騒音形の全閉外扇形主電動機の冷却構造の開発に適用した。その結果、従来の開放形主電動機に対して6dB(A)の低騒音化を達成し、国内初となる早期商品化を達成した。

今後も様々なモータや他製品の開発・設計にこれら熱流体解析技術を適用し、熱設計フロントローディングの展開を行っていく予定である。

参考文献

- (1) 羽下誠司, ほか: パソコン版熱流体回路網シミュレータMelTHERFY/TherfBENCHの開発, 平成12年電気学会全国大会講演論文集(4), 1909~1911 (2000)
- (2) 兼井延浩, ほか: 全閉主電動機の製品化適用技術, 三菱電機技報, 78, No.12, 817~820 (2004)
- (3) 菊池 昇: ファーストオーダーアナリシス, 豊田中央研究所R&Dレビュー, 37, No.1, 1~36 (2002)

車載用デジアナ混載LSI

田中淳也*
岩上祐希**

Digital-Analog Mixed Signal LSI for Automotive Equipment

Junya Tanaka, Yuki Iwagami

要旨

エンジンコントロールユニット(エンジンECU)は、搭載されたメインCPU(Central Processing Unit)により、自動車のエンジンを制御する装置であり、最適な制御によって排気ガスのクリーン化と燃費の改善に寄与している。この装置はメインCPUのほかに、各種デジタル、アナログ部品で構成されており、これらデジタル・アナログ部品を集積化したシステムLSI(Large Scale Integration)を開発した。

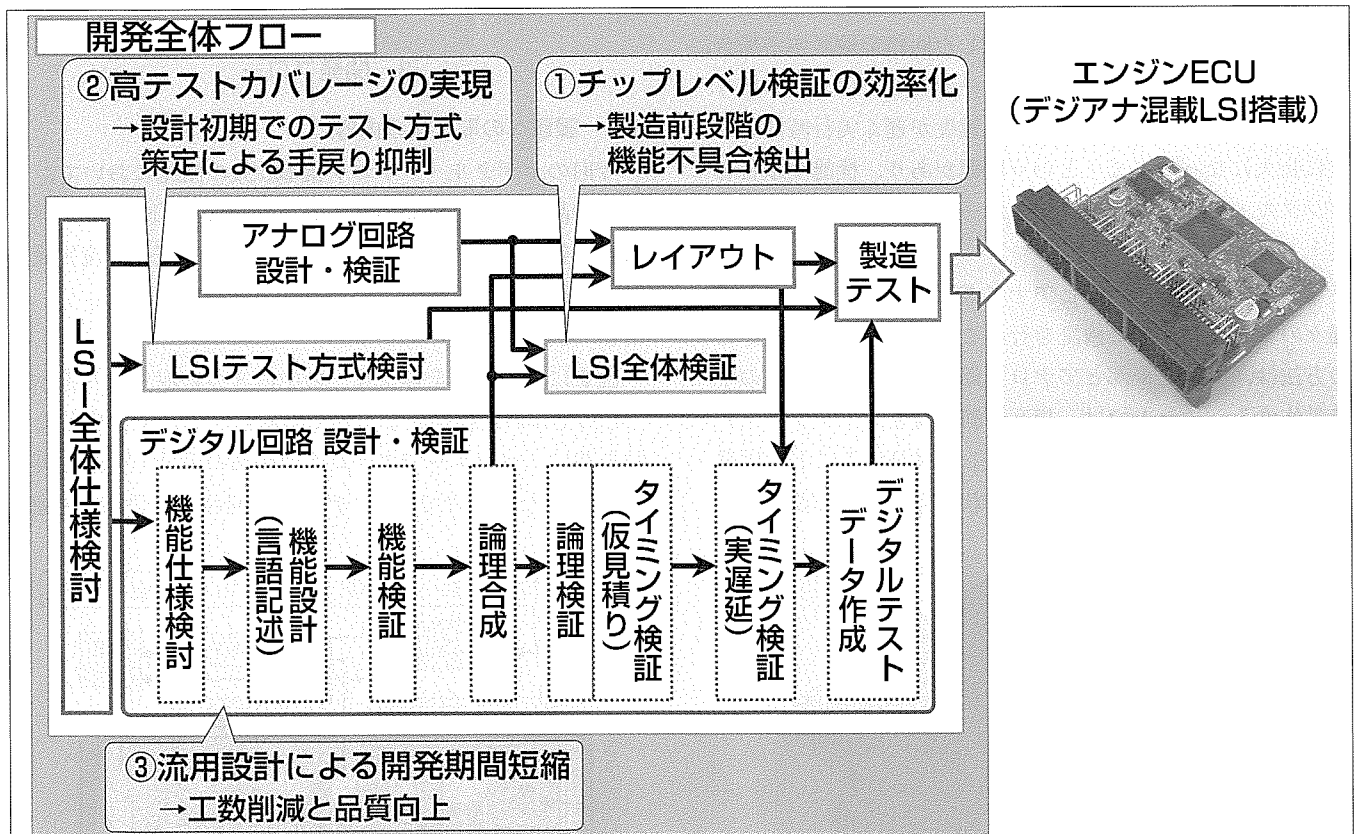
この開発では、デジタル・アナログ回路を混載したLSI開発における設計品質の向上と開発期間短縮を目的に、設計のフロントローディング化によるQCD(Quality, Cost, Delivery)改善に取り組んでいる。

本稿では、“2種類の検証手法を適用したチップレベル

検証の効率化”“設計上流での量産テストを意識した回路検討実施による高テストカバレッジの実現”，及び，“流用設計を意識した回路設計の取り組みによる開発期間短縮”の3点について述べる。

この取り組みで、デジタル機能シミュレータ及びデジタル・アナログ混載シミュレータそれぞれの利点を生かした2つの検証方法の組合せにより、検証の網羅度を高めることができ設計品質を向上させた。また、設計の上流においてデジタル・アナログ回路の接続部の量産テストを意識した仕様検討・回路設計に取り組み、開発の手戻りを抑止し、同時に、高いテストカバレッジを実現した。さらに、流用を意識した回路ブロックの分割設計に取り組むことにより設計期間を短縮させることができた。

特集 II



デジタル・アナログ混載LSI開発フロー中でのQCD改善への取り組み

デジタル・アナログ混載LSIの開発において、その設計品質向上と開発期間短縮を目指したQCD改善として、LSI全体検証の中で①チップレベル検証の効率化、設計上流でのLSIテスト方式検討の中で②高テストカバレッジの実現、デジタル回路の設計・検証において③流用設計による開発期間短縮という3つの取り組みを実施した。

*設計システム技術センター **姫路製作所

1. ま え が き

エンジンECU(図1)は、搭載されたメインCPUにより、自動車のエンジンを制御する装置であり、最適な制御によって排気ガスのクリーン化と燃費の改善に寄与している。この装置は、メインCPUのほかに、各種デジタル・アナログ部品で構成されており、これらデジタル・アナログ部品を集積化し、同時に安全性機能を搭載した第一世代システムLSIを2001年に開発した。そして、今回、更なる回路集積化と、半導体プロセスの微細化によるチップサイズダウン及び原価低減を目的として、デジタル回路とアナログ回路を混載した第二世代のシステムLSIを開発した。

このLSI開発では、デジタル・アナログ回路を混載したLSI開発における設計品質の向上と開発期間短縮を目的に、設計のフロントローディング化によるQCD改善に取り組んだ。

本稿では、2種類の検証手法を適用したチップレベル検証の効率化、設計上流での量産テストを意識した回路検討実施による高テストカバレッジの実現、及び、流用設計を意識した回路設計の取り組みによる開発期間短縮の3点の取り組み内容について述べる。

2. 車載用デジタル・アナログ混載LSIの技術的課題

デジタル部、アナログ部を混載した回路を検証する場合、デジタル・アナログ混載シミュレーションでは、取り扱うアナログ値の解像度にもよるが、速度が遅く実行時間が非常に長大になってしまうという問題があり、機能全項目をデジタル・アナログ混載シミュレータで検証することは事実上不可能である。

このため、デジタル部とアナログ部をそれぞれ分離して、個々のシミュレータで検証を行うことが多い。しかし、この方法は、デジタル部とアナログ部が密接な制御関係の中で動作するシステムでは、相互の制御機能・インタフェース回路に関して十分に全体を網羅して検証することが困難な場合があり、このため、検証漏れを発生させる要因とも

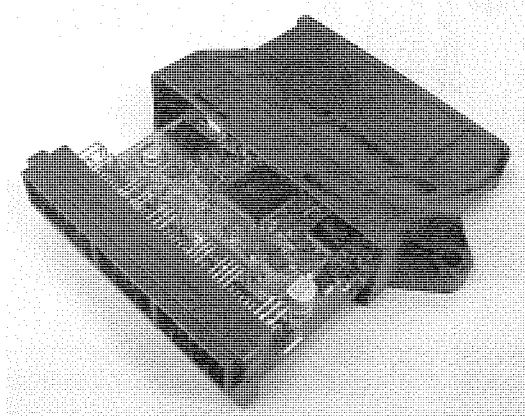


図1. エンジンECU

なる。

今回の開発では、三菱電機内でデジタル部・アナログ部共に回路設計することが望ましかったが、アナログ回路部を当社で設計するには、その半導体プロセスの持つ個々の設計パラメータ及び設計環境をベンダーから開示してもらう必要がある。また、開発期間を短縮させる点も考慮に入れ、所有する半導体プロセス独自の特性などを充分把握しているベンダーの設計専門者に任せることとした。そして、LSI全体の仕様検討とデジタル部の回路設計を当社で実施した。アナログ回路ブロックはベンダーで設計し、デジタル回路ブロックは当社で設計するため、両ブロック間のインタフェース信号の仕様を双方で間違えると、LSI全体の動作として不整合が生じてしまう。設計品質を向上させるためにも、デジタル部とアナログ部を合わせたチップ全体レベルでの機能検証を実施し、開発の上流での不具合の検出に努める必要がある。

また、テスト設計に関しても、デジタル回路部・アナログ回路部の個々のブロックのテストについては、ベンダーと当社でそれぞれ量産テストを考慮した回路設計を進める。そして、同時に、アナログ回路部とデジタル回路部間のインタフェース回路部も、テストできない回路が含まれないように、開発の当初からテスト方法を考慮に入れた回路設計を進める必要がある。

3. 開発フロー

3.1 課題への取り組み内容

今回のデジタル・アナログ混載LSIの開発において、その設計品質向上と開発期間短縮を目的に、①チップレベル検証の効率化、②高テストカバレッジの実現、③流用設計による開発期間短縮の3つの取り組みを実施した。

3.2 開発の全体フロー

図2に示す開発全体フローの中に3つの取り組みを示す。LSI全体の仕様検討を当社で実施し、ここで確定した仕様を基に、ベンダーでアナログ回路部の設計・検証を実施する。また、当社では、“デジタル回路部の設計・検証”

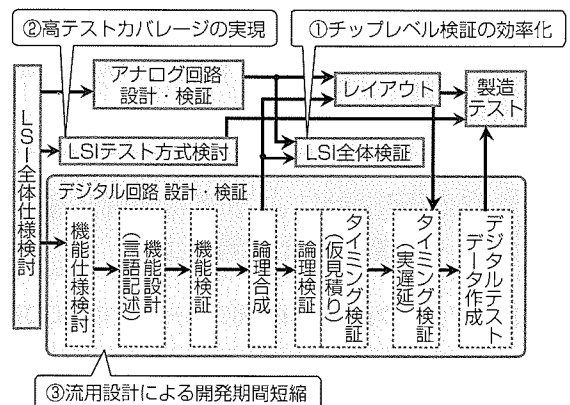


図2. 開発全体フロー

を実施する。並行して、ベンダーと当社共同で、“LSIテスト方式検討”を実施し、これをそれぞれの設計に反映する。個々の回路検証後に、“LSI全体検証”を実施し、問題なければシリコン上への回路レイアウト、製造工程へ移行する。

LSI全体検証の中で①チップレベル検証の効率化を、LSIテスト方式検討の中で②高テストカバレッジの実現を、そして、デジタル回路部の設計・検証の中で③流用設計による開発期間短縮に取り組んだ。

4. QCD改善の取り組み

3つの取り組みに関して、以下に詳細を述べる。

4.1 チップレベル検証の効率化

開発したLSIの全体ブロック図を図3に示す。複数のアナログ回路ブロックにデジタル回路ブロックが囲まれた構造となっている。

今回、回路仕様を効率的に検証するため、目的を大きく2つに分け、2種類の手法で回路を検証し、検証の網羅度を上げて設計品質を高めた。同時に、設計の上流で仕様・回路のバグを検出することができ、設計の手戻りを防ぐことにより、チップレベルでの回路検証期間を短縮した。

まず、一つ目の検証手法では、デジタル機能シミュレータを使用した。ここでは、LSIチップレベルでの詳細機能動作を検証するために、アナログ回路部をデジタルモデル化し、チップ全体をデジタル回路として扱い、高速な機能シミュレータ上で機能検証を実施する手法をとった。これにより、LSI全体の詳細機能確認が高速に実施できた。アナログ回路を設計するベンダー側に回路のデジタルモデル化を依頼することにより、モデル化の信頼性(実アナログ回路との動作の一致性)を高め、同時に検証の精度を高めた。

また、ベンダー作成のデジタルモデルを当社設計のデジタル回路と接続し動作確認することにより、当社が提示したアナログ回路仕様をベンダー側が正しく理解しているかどうか確認できるというメリットもあった。

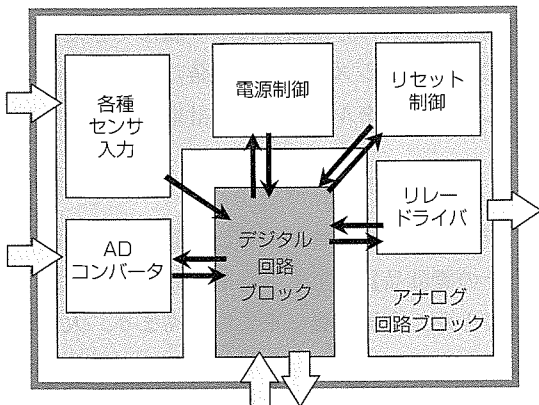


図3. LSIの回路ブロック図

図4に、アナログ回路部のデジタルモデル化の例を示す。複数のアナログ入力値を特定のタイミングでサンプルし、この入力条件により3ビットのCMOS(Complementary Metal-Oxide Semiconductor)デジタル信号を出力する回路がある。アナログ入力信号をデジタル機能シミュレータで扱えるデジタル信号に置き換え、これを制御し、3ビットのデジタル出力を制御するようにしている。

二つ目の検証手法では、LSIベンダーが所有するデジタル・アナログ混載シミュレータを使用した。

デジタル・アナログ混載回路のシミュレーションは、取り扱うアナログ値の解像度を高めると、実行速度が低下し、シミュレーション時間が非常に長大になってしまう。そこで、すべての検証項目に適用するのではなく、実回路におけるデジタル・アナログ回路間の接続確認にねらいを定めて検証を実施した。これにより、デジタルモデルを用いた一つ目の検証手法では盲点となり得る実回路としてのブロック間接続検証を実現した。

以上の2つの手法の組合せにより、検証の網羅度を高めることができ、設計品質が向上すると同時に、検証期間を短縮した(図5)。

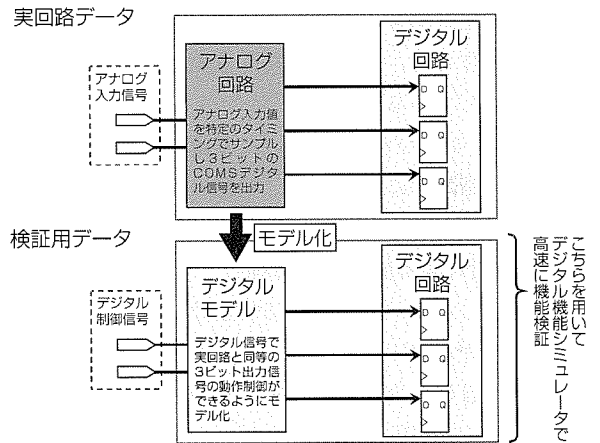


図4. アナログ回路のデジタルモデル化

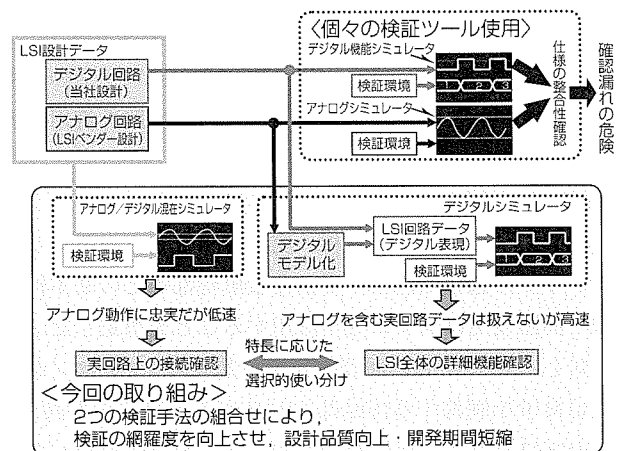


図5. 2つの検証方法による効率化

4.2 高テストカバレッジの実現

このLSIは、エンジンECU上でエンジンの制御に直接かわかるLSIであり、不良品の市場流出を確実に防がなくてはならない。このため、LSIの量産テストには高テストカバレッジが要求される。

アナログ回路は、回路ブロックごとにテストモード時に外部から入出力端子を制御/観測するパスを設け、これを用いてテストするようにした。また、デジタル回路部は、完全同期回路として構成し、フル・スキャンパス・テストで内部回路をテストするようにした。

デジタル回路とアナログ回路の接続信号部分は、LSI内部で閉じていて外部から制御/観測が困難な信号が多いため、設計時に何も対策を講じていないとテストのできない回路が出来上がってしまう。そこで開発の当初で接続回路部分を考慮したテスト方式を策定し、後工程におけるテストのための回路変更手戻りが発生しないよう設計を進めた。テスト方式の例を図6に示す。

アナログ回路ブロックにサーマルシャットダウン回路が内蔵されており、異常過熱を検出すると回路の動作が停止する。同時に、Fault情報がデジタル回路部に伝わる。量産テストでは、この回路ブロックを異常過熱させることはできない。したがって、デジタル回路部にサーマルシャットダウン回路を制御する信号を設けて、量産テスト時にはこの信号を動作させ、このFault信号の動作テストを実施できるようにしている。

このように、設計の上流において量産テストを意識した仕様検討・回路設計に取り組み、開発の手戻りを抑止し、同時に高いテストカバレッジを実現した。

4.3 流用設計による開発期間短縮

当社で実施したデジタル回路部の設計に関して、今回の第二世代システムLSI開発では、第一世代開発の設計/検証データを流用し、設計期間の短縮を図っている。第一世代システムLSIの開発時に、機能ブロックごとに回路を分割して設計しただけでなく、流用設計することを見込み、“完全流用を想定したブロック”と“改訂を予想したブロック”とに分け、機能拡張がしやすい回路構成にしている。

図7に示すとおり、完全流用を想定したブロックの一部において修正箇所も発生したが、大部分は回路を流用することができた。

回路の例を図8に示す。このLSIは、マイコンとのシリアル通信で受けた命令を解析・実行する機能を内蔵する。このシリアル通信機能部や受信命令解析部などの基本機能部は、回路変更はせずに完全流用することを想定した。これに対し、あらかじめ回路改訂を予想した“マイコンからの受信命令を制御する回路部”や“内部レジスタの制御部”などのブロックは、新たな命令やレジスタなど追加した場合に、大きな回路変更を伴わずに機能追加するような工夫

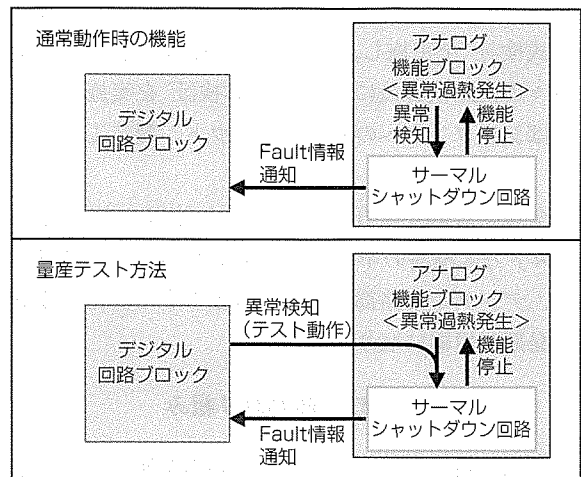
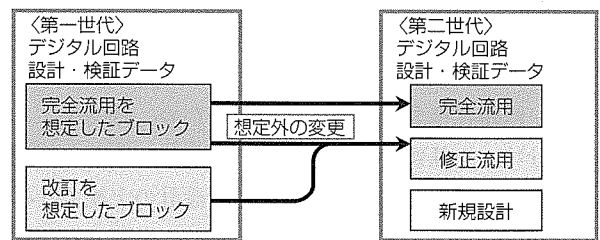


図6. アナログ部とデジタル部の接続信号のテスト例



前回の開発時に“流用設計を意識した回路ブロック分割設計”実施
→今回、その成果の刈り取り

図7. 回路の流用設計

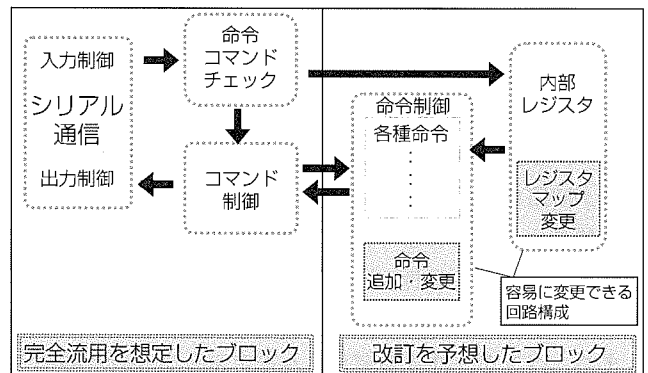


図8. 流用設計回路の例

をしている。

このように、第一世代システムLSI開発時から流用を意識した回路ブロックの分割設計に取り組んできたことにより、今回の第二世代システムLSI開発において、その成果の活用として、デジタル回路部の設計期間短縮を実現した。

5. むすび

今回、デジタル・アナログ混載LSI開発のQCD改善に取り組み、その設計品質向上と開発期間短縮という効果を得ることができた。今後、更に重要性が高まり、大規模及び高機能化するアナログ・デジタル混載LSIの開発をベンダーと共同で取り組む中で、回路全体の設計効率向上を目指し取り組んでいく。

大型映像装置における Gbps高速信号設計技術

島崎 睦*
高島一樹**
諸岡史久**

Gbps, High Speed Signal Integrity of Large Visual Display Controller

Mutsumi Shimazaki, Kazuki Takabatake, Fumihisa Morooka

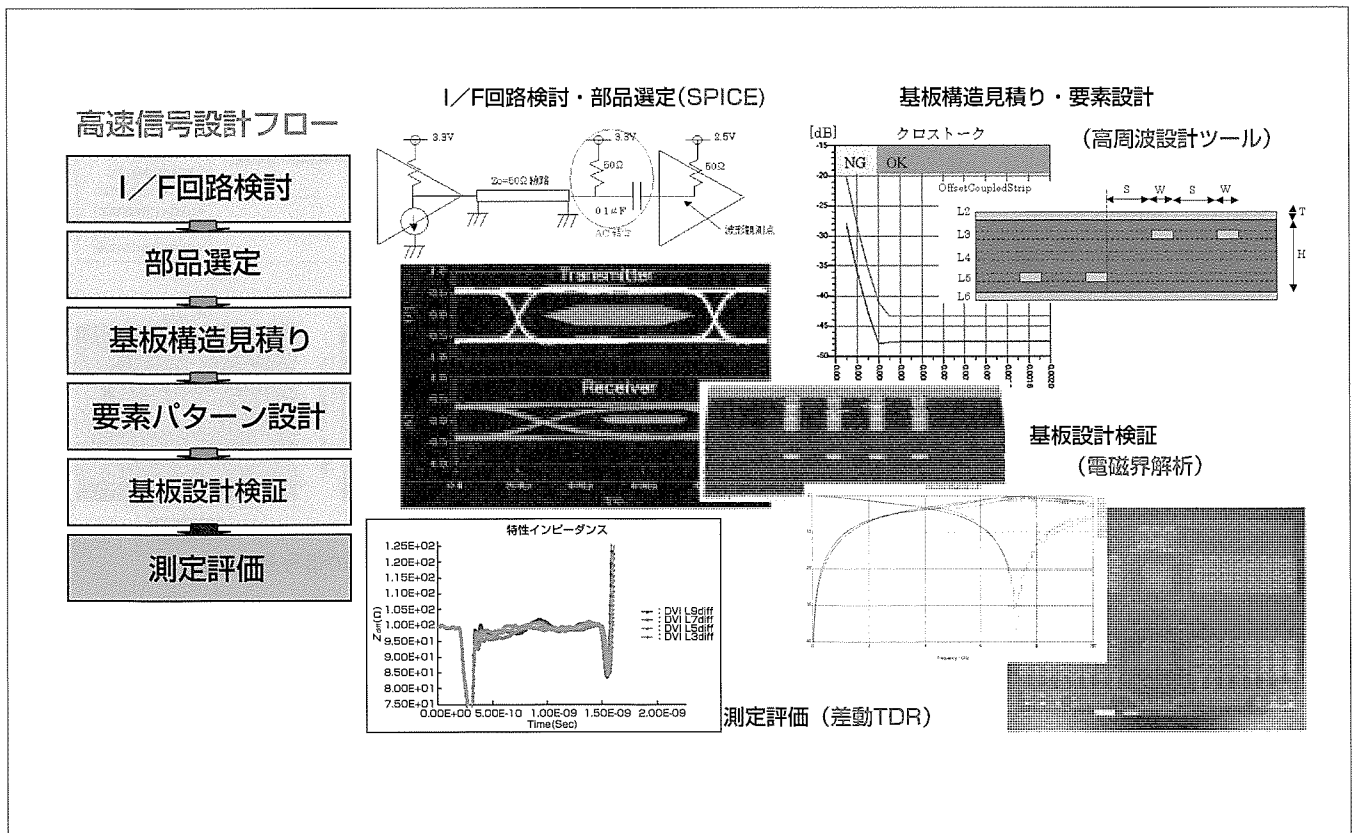
要 旨

三菱電機では、複数画面表示のマルチビジョンや超大型のオーロラビジョン等の映像情報制御機器開発において、システムの小型統合化を進めている。そのための鍵(かぎ)となるのがデジタル映像配線の基板(バックボード)化である。DVI(Digital Visual Interface)規格における伝送レート1.65Gbpsの高速信号を従来ケーブルよりも電気特性の劣るプリント配線板で伝送するには設計品質の向上が必要であり、かつ、従来の開発工期で設計を実現するには、CAE(Computer Aided Engineering)を用いて設計見積り・検証を前倒しに実施するフロントローディング設計が要(かなめ)となる。

本稿では、DVI信号の基板配線設計について、Gbps信号設計に要求される技術と、CAEによる設計・検証を実施して信号品質を確保した例について述べる。

Gbps伝送の設計技術の特徴は、①数百MHz～数GHzま

での超広帯域設計、②時間軸波形と周波数特性の両性質での評価検証である。また、回路では差動信号・電流駆動の設計、基板ではカップルドライン・結合ビア/パッドの構造設計が必要となり、その設計パラメータは従来の約3倍に増加する。DVI信号の設計では、回路シミュレータ(SPICE)による回路インタフェース検証、高周波設計ツールによる基板構造見積り、電磁界解析による要素パターンモデリング、及びそれらの総合解析による基板設計検証を実施し、300mm×430mmのバックボードを製作した。特性測定による評価結果は、差動インピーダンス・アイパターンとも設計見積り値や検証結果と良く一致し、設計段階での信号品質の作り込みを従来工期で実現できた。今後、Gbps信号伝送の要求は増加することが予想され、設計スタイルの定着と技術蓄積が製品品質向上に大きく貢献するものと確信する。



高速信号設計の設計項目とCAEツールの適用

Gbps高速信号設計で行われる設計手順に対し、その項目に最適なCAEツールを使い分けることで、従来開発工期のまま信号品質を作り込むことが可能となる。また、測定評価を考慮に入れた設計が、測定の精度や機能評価の効率を改善する。

1. ま え が き

近年、プラズマディスプレイや液晶ディスプレイに代表される映像表示装置の大型化・高精細化の製品要求は高く、その進化の要は映像信号のデジタル化と言える。こうした中、UXGA(Ultra Extended Graphics Array)やHDTV(High Definition Television)のような高解像度表示モードの品質を犠牲にすることなくデジタル信号の直接伝送を実現したのがDVI規格⁽¹⁾である。DVIは情報密度の高い映像信号をケーブル伝送するため、その伝送レートは最高1.65Gbpsにまで及び、現在の主流といえるGbpsシリアル伝送方式の一つである。

当社製品においては、公共施設向け用途のマルチビジョン(複数画面による映像表示装置)やオーロラビジョン(超大型映像表示装置)等の大型映像制御システムでもDVIを採用している。しかしながら、複数の機器で構成されるこれらのシステムは、システムサイズ(大きさ)やケーブル配線によるメンテナンス性の課題を抱えてきた。新製品の開発では、これらの課題を解決するため機器の統合化を図り、従来のケーブル配線をバックボード配線で実現した(図1)。伝送特性の劣るプリント配線板で高速なDVI信号の品質を確保するために、CAEを活用した設計見積り・検証作業を前倒しに実行するフロントローディング型設計を適用した。

2. DVI規格における信号品質

DDWG⁽¹⁾により制定されたDVI規格の中で、伝送信号の品質にかかわる規定の概要を次に示す。回路方式はT.M.D.S(Transition Minimized Differential Signaling)と呼ばれるCML(Current Mode Logic)のインターフェースであり、定電流源と終端抵抗による差動駆動である。終端抵抗 $R_T=50\Omega \times 2$ で電圧振幅は $\pm 500mV$ となり、ケーブルインピーダンスは差動 $Z_{diff}=100\Omega$ で整合する。映像信号の伝送レートは最大1.65Gbpsで、画面解像度に依存しSXGA(Super XGA)のLCD(Liquid Crystal Display)表示でも実質は1Gbpsを超える。信号の品質は伝送波形のアイマスクにより、振幅とジッタが定義され受信可能振幅は $\pm 75mV$

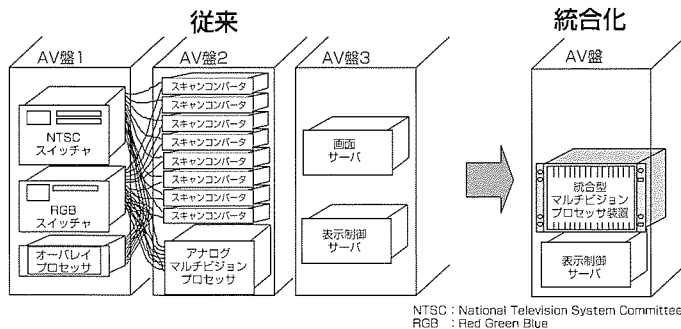


図1. システムの統合化によるバックボード配線の実現

以上、ジッタ許容は0.25UI(片側)から1Gbpsでのマスク幅は500ps以上である。外部機器との接続に必要な認定試験を通すためにはこのマスクをクリアすることが要求される(図2)。

3. 基板配線によるGbps信号伝送の実現

一般的なガラスエポキシ材料(FR4)を用いたプリント基板配線では、材料の電気的な特質により、伝送用途に作られたケーブルの持つ高品位な信号波形は望めない。また、システム機能評価時にバックボードではケーブルのように相性の良い特性のものに容易に取り替えることができないため、基板製造前の十分な検討が不可欠である。Gbps伝送の設計技術の特徴は、

- (1) 数百MHz(DC)~数GHzまでの超広帯域設計
 - (2) 時間軸波形と周波数特性の両性質での評価検証
- であり、デジタル回路設計とマイクロ波回路設計を融合した新たな技術要素が要求される。また、回路設計では差動信号・電流駆動の設計技術、基板設計にはカップルラインと結合ビア/パッドの設計技術が不可欠である⁽²⁾。基板設計での検討要素を抽出すると、数百Mbpsまでのデジタル信号の設計配慮パラメータに対し、数Gbpsのシリアル伝送で考慮すべき基板設計パラメータは約3倍に増加する(表1)。こうした技術要素の増加に対し信号品質を確保す

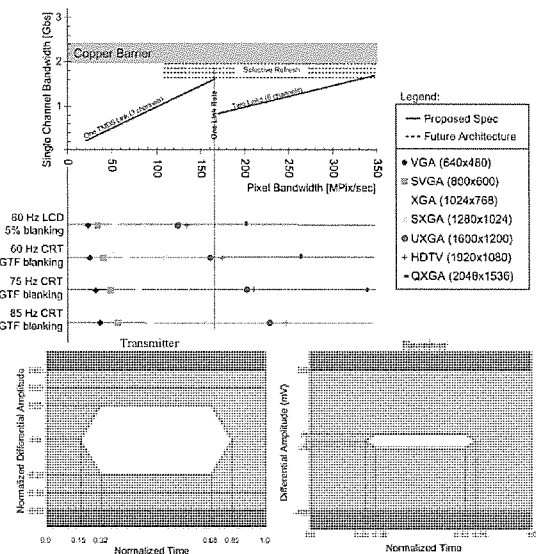


図2. DVI信号の信号品質定義⁽¹⁾

表1. 基板設計パラメータ(下線: Gbps設計で追加)

- (1) 基板材料: 導電率 σ , 誘電率 ϵ_r , 誘電正接 $\tan \delta$, 表面粗さ
- (2) 層構成(断面): 絶縁層厚 H , 配線導体幅 W , 配線導体厚 t (めっき厚), 差動間隔 g , レジスト厚
- (3) 配線制約: 配線間隔 s , 配線長 L , 差動間隔路長差skew, 引出し単線長 d
- (4) レイアウト: 曲げ方(45°, ベンド, 凹), 半径 r , 曲げ角 θ
- (5) 層渡り: スルーホール(via長, via径, ランド径, クリアランス径, めっき厚), viaスタブ長
- (6) GND: GNDvia間隔, パソコン配置

るには、設計時における見積りと検証を計画的に実施し、**図3**に示すフロントローディング型設計フローを実践することで、開発の手戻りを最小に抑えることができる。ただし、見積りや検証を従来工期で実現するにはCAEによるシミュレーション計算が不可欠となる。

4. CAEシミュレーションの適用

Gbps信号伝送の設計項目は、回路インタフェース検討、部品選定、基板構造見積り、要素パターン設計、基板設計検証の手順となる。各設計項目に対し共通して活用できるCAEツールは回路シミュレータのSPICEであり、最近のSPICEは、等価回路の計算だけでなく、2D電磁界解析ソルバーによるWエレメントやSパラメータモデル、アイパターン表示機能を含み、Gbps信号の解析に対応できる。しかし、物理構造のモデル化や周波数特性・アイパターンの見積りには、高周波設計ツールや電磁界解析ツールの方が容易かつ正確に計算できる場合が多く、目的に合わせた使い分けで検証効率と精度を上げられる。部品選定や基板構造見積りには高周波回路設計ツール、要素パターンモデリングには電磁界解析、回路インタフェース検討と基板設計検証にはSPICEを用いたDVI信号設計の内容を述べる。

4.1 SPICEによる回路インタフェース検討

異種電源のチップ間をDVI伝送する場合、DCをカットする必要からAC結合を検討する必要が生じる。1.65GbpsのDVI信号におけるSPICEによる検証結果を**図4**に示す。0と1の非対称性のあるデジタル信号では、バイアス電圧の変動が生じるため、AC結合ではアイマスクをクリアしない時間が存在している。また、DCバイアスを決める抵抗の接続により終端インピーダンスが不整合になる影響もSPICEによる計算で確認した。

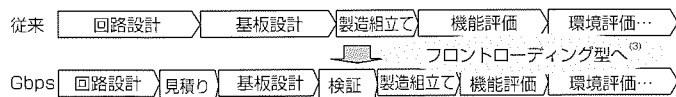


図3. フロントローディングした設計スタイル

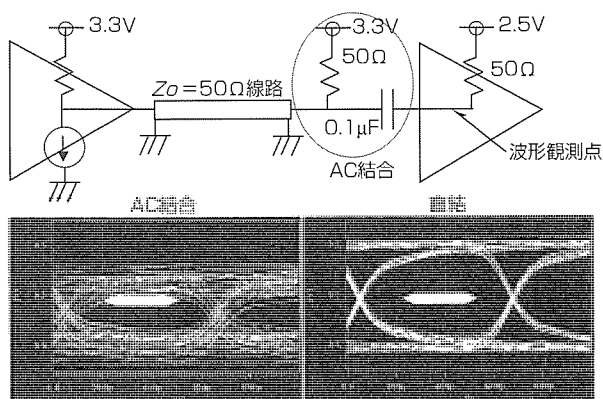


図4. SPICEによるI/F回路の計算

4.2 高周波設計ツールによる基板構造見積り

Gbps信号を伝送する基板配線では、差動インピーダンスやクロストークをコントロールする必要がある。基板配線の見積りには半導体デバイスのSPICEモデルを必要とせず、基板断面構造パラメータの変更が容易に可能な高周波設計ツールを活用した。インピーダンス計算した断面構造のパラメータを変化させて伝送損失やクロストーク特性を見ることがオフセットカップルドストリップラインのように複雑なクロスセクションを最適化した**図5**。

4.3 電磁界解析による要素パターンのモデル化

基板構造の中でGbps信号へ影響を与える要素として、配線の曲げや、コネクタやLSI(Large Scale Integration)パッケージを実装するためのビアとパッドがある。これらの要素パターンは三次元構造として特性を把握する必要がある。電磁界解析での特性計算を実施した。**図6**はこのバックボードの層構成における多ピンコネクタ実装部の解析結果である。貫通型ビアと配線の接続について、コネクタ実装側配線層(C面)と反対側(S面)での引き出しによる周波数特性を見たものである。C面引出しはビアが分岐(スタブ)となり並列共振による特性劣化がみられる。この特性を示すSパラメータを次節に示すアイパターン計算のモデルに用いれば、信号品質に与える影響を確認できる。

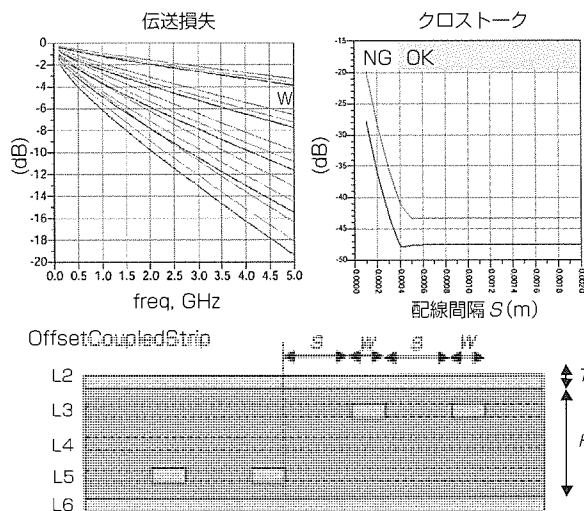


図5. 基板クロスセクションの見積り

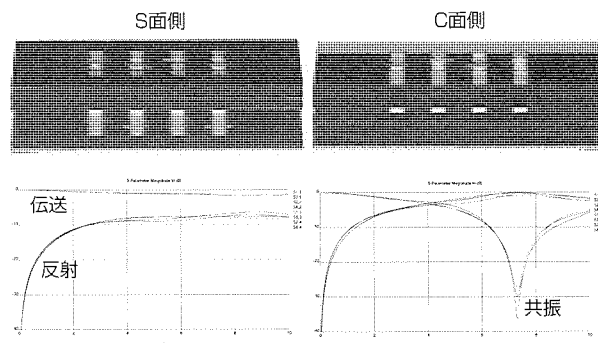


図6. コネクタ部の電磁界解析

4.4 SPICEによる基板設計検証

最終的な基板設計の検証には、半導体デバイスのSPICEモデル、基板クロスセクションのWエレメント、コネクタピアやパッドのSパラメータをモデルとしたシステムアイパターンの計算をSPICEで実施する。4.3節で示した引出し層による周波数特性差は、DVI信号の1.65Gbpsの信号品質としてはジッタで数ps程度の差であり、バックボードサイズ(300mm×430mm)を想定した基板線路長のシステムとしても十分にマスクをクリアすることを確認した(図7)。

5. 測定評価

十分な設計検証の下で製作された製品でも、品質を評価するための特性測定は重要な作業である。ただし、Gbps信号に対しその特性を正確に測定するのは容易ではなく、高価な専門の測定器を必要とするのみならず、Gbps伝送設計技術についての理解が必要である。特に考慮が必要なのはプロービングの方法であり、プロービングによる測定を念頭に置いた設計が機能評価の期間短縮に結び付く。この報告の例では、特性測定のための評価用配線を基板にレイアウトし、マイクロ波プローバや差動プローブのピッチに合わせたパッド配置やピン配置を行い、特性把握の高精度化と効率化を実践した。

今回製作したバックボード基板と、差動TDR (Time Dmain Refractometry)測定値を図8に示す。差動インピーダンス Z_{diff} は全高速配線層において $100\Omega \pm 7\%$ という良好な結果が得られた。また、バックボードへの映像信号入出力に5mのDVIケーブルを接続し、パソコン出力のLCD入力におけるバックボードの受信、送信をコネクタピンで測定した結果を図9に示す。試験的な波形測定にもかかわらず受信マスクをクリアする良好なアイパターンを得ることができた。信号入出力用のケーブルを外した本来のシステムでは、検証結果に近い高品位なアイパターンが得られると推測できる。

6. むすび

大型映像制御システムの統合化におけるバックボード配線のDVI信号伝送設計について、CAEツールを活用したフロントローディング型設計を実践し、技術要素の増加したGbps信号伝送基板を、試作レスかつ従来設計工期で実現した。高速シリアル伝送の分野としてはデジタル映像信号のみならず、DVI信号(1.65Gbps)を上回る信号レートの基板伝送の要求が増加すると予想され、この設計スタイルの定着とGbps伝送設計の技術蓄積が、製品品質の向上につながるものと確信する。

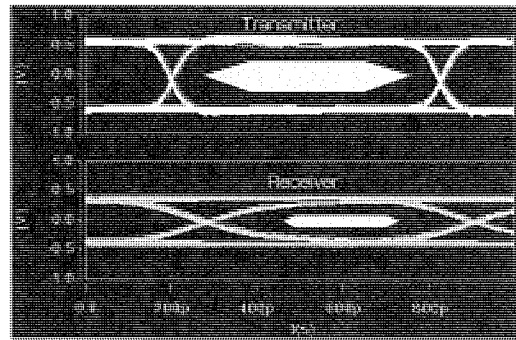


図7. バックボードシステムでの波形検証

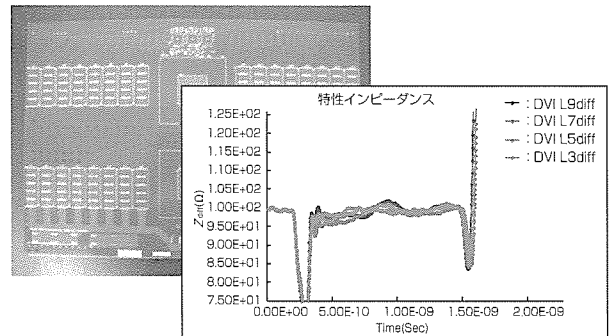


図8. 製作したバックボードとTDR測定値

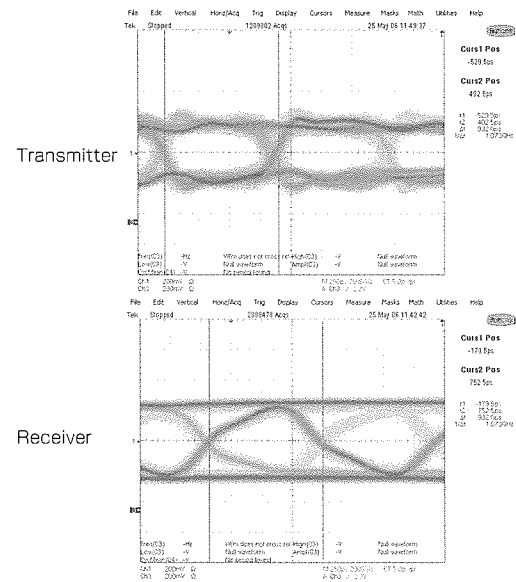


図9. 波形測定結果

参考文献

- (1) DigitalDisplayWorkingGroup : Digital Visual Interface DVI Revision 1.0 (1999)
- (2) 田中顕裕 : 高速差動伝送に対応したプリント配線板パターン設計の実際, エレクトロニクス実装学会誌, 8, No.4, 271~276 (2005)
- (3) 中岡邦夫, ほか : 製品設計の現場で使うフロントローディング設計, エレクトロニクス実装学会誌, 7, No.7, 564~568 (2004)

ASIC/FPGAの機能検証技術

上野 仁*

A Functional Verification Method for ASIC and FPGA

Hitoshi Ueno

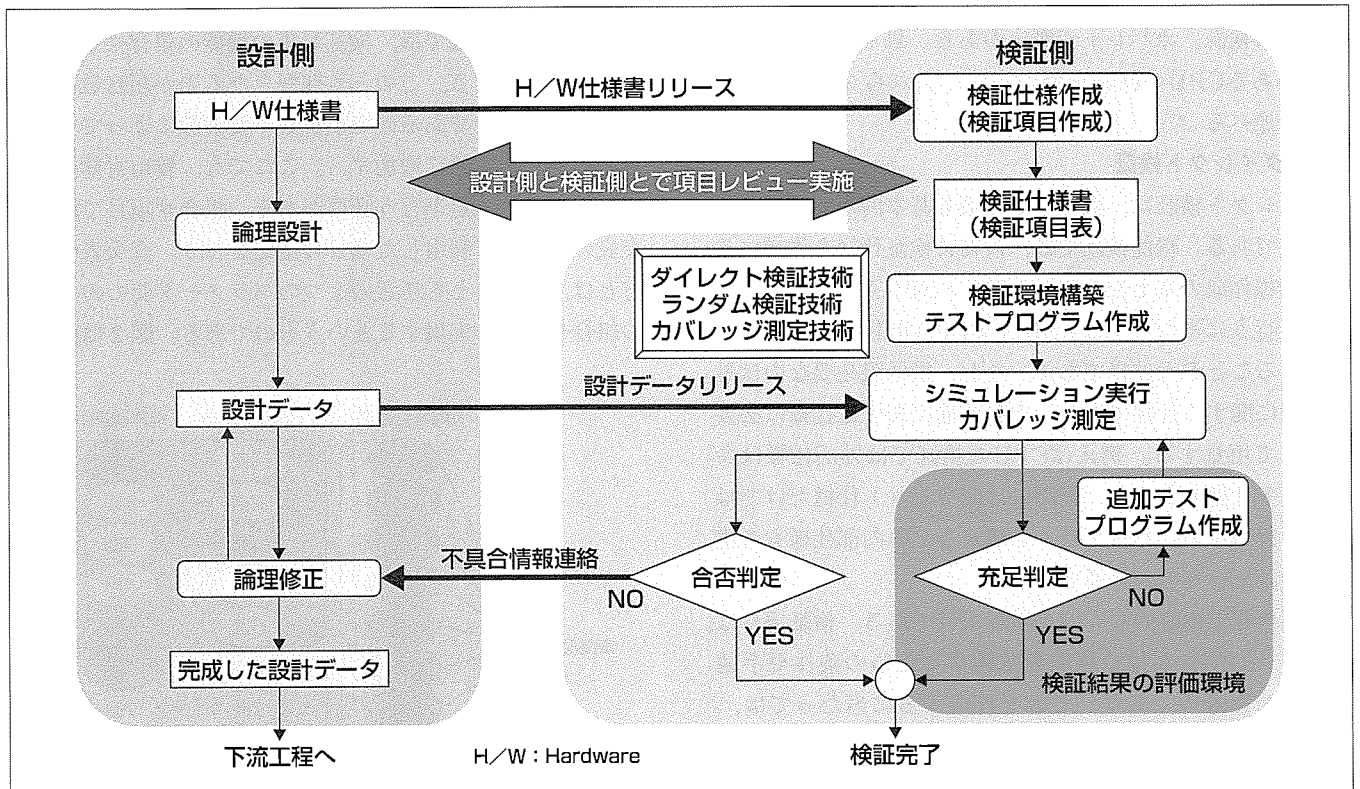
要旨

デジタル機器のキーパーツであるASIC (Application Specific Integrated Circuit) / FPGA (Field Programmable Gate Array)の開発では、半導体の微細加工技術の進歩に伴い集積可能な素子数が増大しており、搭載可能な機能も増大し高機能化・複雑化している。このために、論理設計の負荷増大に加えて、機能検証負荷の増大が顕著である。このような背景の下、論理設計段階での機能不具合の除去が不十分となり、開発下流であるレイアウト設計段階や製造段階、又はフィールドにおいて致命的な不具合が見付かるおそれが増大している。製品開発フローの中で見付かる不具合の除去にかかるコストは、下流になるほど増大する。ASICを再作成する場合、最先端プロセス(90~65nm)を使用するとマスク費用として数億円が必要である。また、フィールドで不具合が見付かった場合には、社会的

信用の失墜やブランド力の低下など、重大な影響を及ぼす。このような状況により、ASIC/FPGA開発における機能検証の重要性が増している。

本稿では、ASIC/FPGAの品質確保のキーとなる第三者的機能検証技術についてダイレクト検証技術、ランダム検証技術、カバレッジ測定技術といった要素技術を述べた後、現状分析と課題整理を行い、問題解決に向けた取り組みとして検証結果の評価環境について述べる。検証結果の評価環境とは、意図した試験が確実に実施されたことを自動チェックする環境である。この環境を構築し汎用マイコンのCPU(Central Processing Unit)周辺回路検証に適用した結果、テストプログラムの試験条件漏れを検出し検証漏れの防止に効果があることを確認した。

特集 II



第三者的機能検証フロー

論理不具合を論理設計段階で確実に除去するためには、設計者の思い込みや勘違いを排除できるよう、客観性を持った機能検証を行うことが重要である。したがって、機能検証は、検証専任の検証エンジニアを置いた第三者的機能検証フローに従って実施する。

1. ま え が き

ASIC/FPGAの開発では、論理設計段階において十分な機能検証を行い、開発の下流工程やフィールドへの不具合流出を防ぐことが重要である。この機能検証への取り組みは従来から行われているが、近年の微細加工を中心とする半導体技術の進展による回路規模の増大により、設計品質の維持向上が困難になってきている。機能検証負荷は設計負荷と比べて指数的に増加する。これは、機能検証では機能の組合せを網羅した検証を行うのが基本であり、組合せの量が爆発的に増えるからである。そのために検証漏れを起こす可能性が増大しており、結果として、設計品質の維持向上が困難となる。

本稿では、機能検証の要素技術について整理し、課題抽出と対策実施例について述べる。

2. 機能検証の要素技術

機能検証はチップ製造段階以前に行うので、その検証環境はコンピュータ上に擬似的に構築された設計結果のシミュレーション環境であり、設計結果を動作させるためのステミュラスを用意し外部から与えることにより動作させ、その結果をあらかじめ用意した期待値と比較することで合否判定を行うものである。機能検証ではこのような動的な検証が主流であり、その要素技術として、ダイレクト検証、ランダム検証、カバレッジ測定がある。以下に三菱電機で実績のあるCPUの検証を例にして、これら3つの技術について述べる。

2.1 ダイレクト検証

ダイレクト検証は、機能検証で最も基本的かつ重要な検証方法である。機能検証では、最初に検証仕様を作成する。検証仕様作成の基となるのはASIC/FPGAの仕様であり、検証を行うに当たってはASIC/FPGAの仕様が明確になっていることが大前提である。なお、最低限必要なのは外部機能に関する仕様であり、内部機能に関する仕様は必要に応じて用意する。例えばCPUの検証では外部仕様は命令セット仕様であるが、実際には命令セット仕様だけでは検証を行わない。パイプライン構造などの内部仕様も考慮して検証を行うのが普通である。

検証仕様で中心的なものが検証項目である。検証項目は、ASIC/FPGAが持つ機能を試験するための条件や手続きを示したものであり、これを作成するに当たっては、ASIC/FPGAの仕様を正しく理解することが大事である。正しく理解し漏れなく検証項目を作成するための手段として機能系統図や原因結果図などがある。いずれも人間が作成する図表であり、複雑なASIC/FPGAの仕様を体系的に理解し、検証項目を漏れなく抽出するのに効果がある。検証項目を決定した後にテストプログラムを作成しシミュ

レーションを行うが、シミュレーション時間は項目数に比例して増大するので、現実的な期間で検証を完了させるためには検証項目数を抑える必要がある。つまり、重要度に応じて検証項目を取捨選択する。このような考え方に基づいた項目の選定方法として同値分割がある。同値分割とは、ある試験のパラメータが取り得る全要素を尽くすのではなく、要素を幾つかのグループに分割し、個々のグループから代表値を選んで試験を行う方法である。このときグループ分けの方法が大変重要であるが、その基準はASIC/FPGAの内部仕様から決定することが多い。また、グルーピングしたときの隣接するグループの境界にある値は境界条件であり、それらを境界値として試験対象とする。

図1は転送回数を項目として考えた場合の同値分割及び境界値選択の例である。この例では項目の要素数が10であり、それらは2つにグルーピングされている。この2つにグルーピングするという判断は、機能の内部仕様から判断する。つまり機能の実現方式として、転送回数が1~5回までの場合と、6~10回までの場合では論理内部の動作する部分が異なるような仕様であったとする。その場合、1~5の値及び6~10の値はそれぞれ同値とみなすのである。そして、グループ内から代表値として値3と値8を選択している。また同時に、それぞれのグループの境界値として値1, 5, 6, 10を選択している。結果として検証項目は10から6へ削減できる。

検証項目の作成では、検証対象の機能の組合せを考慮した項目を作成する。このとき問題となるのが項目数の爆発である。組合せであるので項目数や要素数によって検証項目の総数が指数的に増加する。ここでも、費用対効果を考慮した項目の決定を行う必要がある。組合せ項目では、直交表の考え方を利用した項目の選定を行う。直交表の考え方は、少なくとも任意の2つのパラメータ間での各要素の組合せ網羅を実現するというものである。図2は直交表

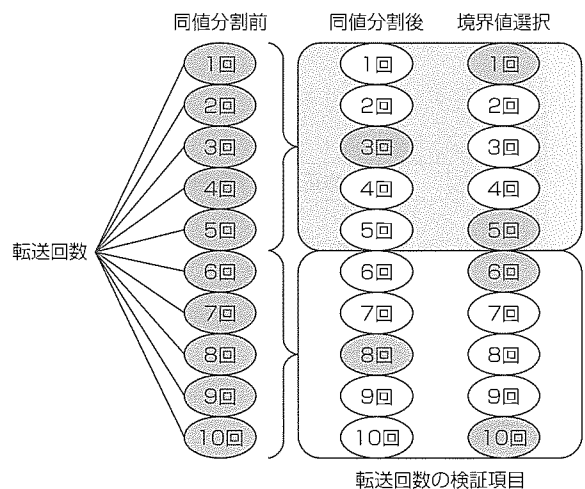


図1. 同値分割及び境界値選択の例

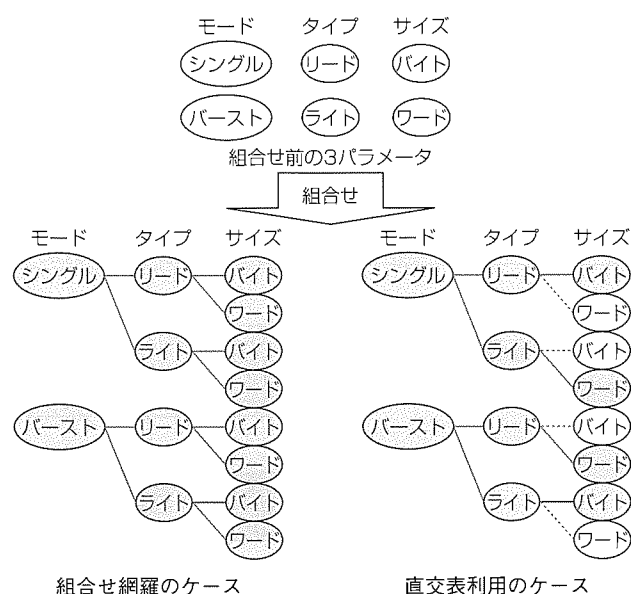


図2. 直交表を利用した項目組合せの例

の考え方に基づいて組合せの項目を選定した例である。

パラメータとしてモード、タイプ、サイズの3つがあり、それぞれは2つの要素を持っている。このようなケースで組合せを網羅した場合には合計8ケースの項目となるが、直交表の考え方をを用いることで項目数は4ケースに削減可能となる。ただし、すべての場合でこの考え方が通用するわけではない。3パラメータ間の網羅が必要かどうかの判断は、仕様から判断して決める。これまでに述べたように、ダイレクト検証では検証項目の選定が大変重要である。漏れがなくかつ現実的な期間で検証が完了可能なボリュームで検証項目を決定することが重要である。

2.2 ランダム検証

ランダム検証は、ダイレクト検証の欠点を補完する目的で生まれた検証方法である。つまり、ダイレクト検証では、検証項目を人間が作成するために、常に項目漏れのおそれが存在する。このヒューマンエラーに起因する検証の漏れを、ランダム生成による偶発性によって補完する。また、ランダム検証では、テストプログラムを自動生成するケースが多く、検証の消化スピードが人依存ではなくマシンリソース依存でリニアに改善するという利点もある。ランダム検証では、検証対象に最適化した専用のツールを自製し利用することが多い。このツールの特徴として2点ある。

(1) ランダムシード値は外部から与える

ランダム生成によって得られたテストプログラムやそのシミュレーション結果は、合否判定において合格となった場合には保存することなく捨てられるのが普通である。したがって、テストプログラム生成の再現性を確保するために、ランダムシード値はオペレータが与えるようにする。

(2) 期待値生成シミュレータを持つ

合否判定のための期待値も自動生成しなければならない。

このために、ランダム生成ツールは、期待値生成のための簡易シミュレータを内蔵することが多い。

ランダム検証では、試験で使用するパラメータ値をランダムに決定するために試験効率が悪いという問題がある。現実の検証では、潜在する不具合は検証対象の全機能の領域に散らばって分布しているのではなく、ある特徴的な領域に偏って潜在していることが多い。したがって、ランダム性だけに頼った検証では潜在する不具合を見付けるには効率が悪い。これを解決するために、ランダム検証であっても外部から試験項目を与える場合が多い。ただし、ここで言う試験項目とはダイレクト検証における項目とは粒度が異なり、大変おおまかな項目である。CPU検証でのランダム生成ツールに与える試験項目の例として、使用する命令やデータ、使用するレジスタ、使用するメモリ領域、キャッシュやアドレス変換機構のオン/オフ、割り込みの有無などがある。いずれも、CPUに特有の機能であるパイプライン制御にかかわる部分の検証を意識した試験項目である。このように、ランダム検証でも大まかな試験項目は存在し、オペレータがそれらの項目を適切に設定することで試験効率の良いランダム検証を実現している。

2.3 カバレッジ測定

機能検証では、策定した検証項目のすべてがシミュレーションによる合否判定で合格となって完了する。しかし、検証項目自体は人間が作成したものであるため、より客観的な検証の完了を示す指標が必要である。そのような指標の1つにカバレッジがある。カバレッジの代表的なものにコードカバレッジがある。コードカバレッジは、シミュレーション実行の結果として設計論理のどの部分がどのように動いたのか、又は動かなかったかをレポートする。コードカバレッジを測定するツールは各EDA (Electronic Design Automation)ベンダーから発売されており、汎用的なツールとして広く使用されている。また、仕様書に明記された機能が検証できているかを測定する機能カバレッジが近年注目されている。

3. 課題と解決に向けた取り組み (検証結果の評価)

前章で述べてきたように、機能検証に対して各種要素技術を用いた取り組みを行ってきたが、ASIC/FPGAに搭載される機能の増大や高機能化・複雑化に対して十分とは言えず、検証漏れを引き起こしていた。不具合の下流工程への流出防止を確実にするために、過去の検証漏れの分析から課題を抽出し解決を図った。

3.1 課題抽出

検証漏れの原因は以下の2つに大別される。

- (1) 検証項目に漏れがあった。
- (2) 検証項目は存在するがテストプログラム及び検証環境に誤りがあった。

一つ目の検証項目の漏れに対しては、図表作成による仕様の正しい理解と検証項目レビューを行うことで対応することとし、同値分割や直交表を用いて検証項目抽出を徹底した。2つ目のテストプログラムや検証環境の誤りによる検証の漏れは、従来から行われているコードカバレッジ測定によって発見できない可能性がある。具体的には、ある機能が設計されずに漏れていて、かつテストパターンでもその機能の試験が漏れていた場合に、コードカバレッジでは検証漏れを検出できない。このために、テストパターンの不備を効率良くチェックできるような仕組みを構築する必要がある。テストパターンの作成を別部門が担当する場合にはこの重要度はより増してくる。

3.2 検証結果の評価手法

前記の問題に対応するために、CPU周辺回路検証に対応したテストプログラムや検証環境の誤りに起因する検証の漏れを検出し防止するための検証結果の評価環境を構築した。この環境を利用することにより、テストプログラム及び検証環境の誤りによる検証の漏れを防止することが可能となる。図3はこの環境のフローを示したものである。

CPU周辺回路検証では、テストプログラムは周辺回路へ試験パラメータを設定するためにアドレス空間にマッピングされた制御レジスタへアクセスを行う。これは、論理の動作としては、バストランザクションという形で観測される。その後、テストプログラムは、周辺回路の起動と終了待ちを行う。これは、試験パラメータの設定時と同様に制御レジスタへのアクセスや、又は特定の信号の変化や割り込み待ちといった動作となる。検証結果の評価環境では、シミュレーション中にどのアドレスにどのような値が読み書きされたか、又はある特定の信号がどのように変化したかを記録しておく。そして、そのアドレス値やストア値、発生したイベントの順番を解析し、どのようなパラメータ値で試験が行われたのかを調べレポートする。DMA (Direct Memory Access) 検証にこの環境を適用した例を図4に示す。この例では、試験漏れとして以下の2ケースが見付かった。

- (1) DCR0が値1のケース：転送カウンタ値が1のケースが漏れていた。
 - (2) DDA0が値FE000000-FEFFFFFFの範囲内のケース：転送アドレスが外部メモリのケースが漏れていた。
- なお、この検証のボリュームは検証項目数で約1,500項目、シミュレーション負荷はSun Blade^(注1)1000でのNC-verilog^(注2)実行で約6時間であり、評価によって増加した実行時間は数%程度であった。

(注1) Sun Bladeは、Sun Microsystems社の登録商標である。
 (注2) NC-verilogは、Cadence Design Systems社の登録商標である。

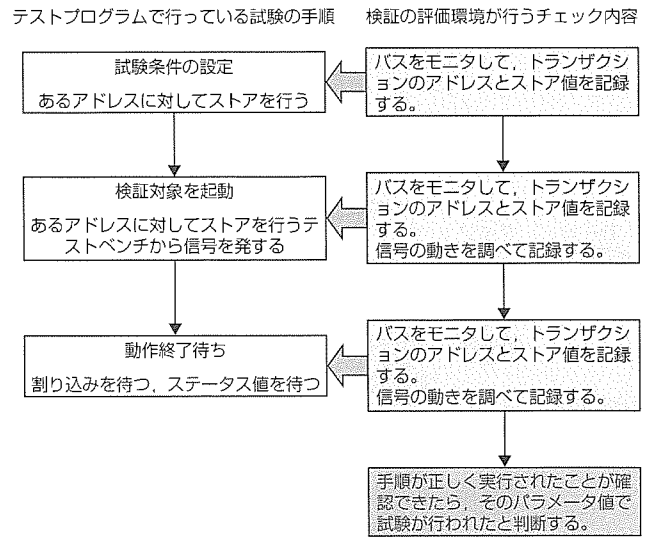


図3. CPU周辺回路検証の評価方法

===== DCR0 =====			
0	0169times	GO	
1	0000times	*** NG ***	
2	0003times	GO	
3<1>0xfffffff	0003times	GO	
===== DDA0 =====			
0x400<1>0x7fff	0168times	GO	
0xFE000000<1>0xFEFFFFFF	0000times	*** NG ***	
0xFF000000<1>0xFEFFFFFF	0016times	GO	
===== DMD0. MD0 =====			
0	0007times	GO	
1	0166times	GO	
3	0002times	GO	

図4. 評価結果ファイル

4. むすび

今回、検証結果の評価環境を構築しテストプログラム作成ミスによる検証漏れの防止に効果があることを確認できた。しかしながら、検証項目の漏れに対しては現状では検出することはできない。今後は、検証項目漏れに対する取り組みを進めていく。また、より上位である仕様自体の検証にも取り組み、ますます大規模化するASIC/FPGAの品質向上に努める。

参考文献

- (1) Bergeron, J.: Writing Testbenches Second Edition, Kluwer Academic Publishers (2003)
- (2) 橋田光弘, ほか: システムLSI応用製品の品質向上をねらいとした検証・テスト技術, 三菱電機技報, 73, No.9, 623~626 (1999)
- (3) 石井康雄: ソフトウェアの検査と品質保証, 日科技連 (1986)



特許と新案 * * *

三菱電機は特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社 知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

熱流体CAEシステム 特許第3780361号(特開2002-304422)

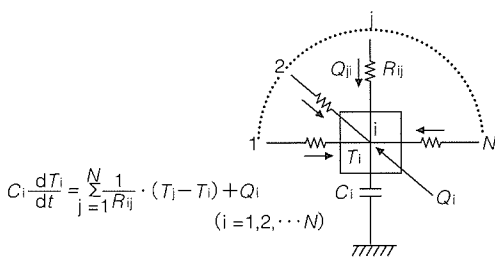
発明者 大串哲朗, 加賀邦彦, 後藤明広, 今泉明子, 小柳正俊, 村上政明

この発明は、機器内の温度、熱流、流体の流量を回路網を用いて計算する熱流体解析CAEシステムに関するものである。この発明に基づき開発した汎用熱・流体解析ソフトウェア及び専用プリポスト処理ソフトウェア(それぞれMelTHERFY, TherfBENCHの商標で三菱電機情報ネットワーク(株)で販売)により、電気回路網をイメージして定常及び非定常の解析を行うことができる。

伝熱問題を解析するときには、物体(流体を含む)の各部を幾つかのブロックに分割し、各ブロックを代表する節点(ノード)を設け、各節点間を熱抵抗で連結する熱モデルを

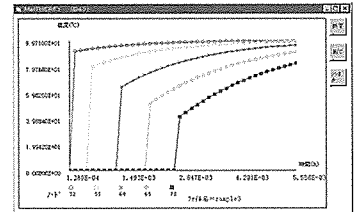
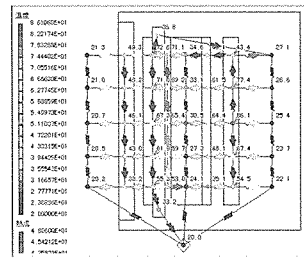
考える。この熱モデルにおいて、各節点間の熱抵抗と各節点を持つ温度と熱容量を用いたエネルギー保存の式を解くことにより、各節点の温度と節点間の熱流を求めることができる。

主な応用分野は、電子機器、重電機器、回転電気機器、工作機械、金型、熱交換機などにおける加熱、冷却、熱交換能力解析である。



$$C_i \frac{dT_i}{dt} = \sum_j \frac{1}{R_{ij}} \cdot (T_j - T_i) + Q_i \quad (i=1,2,\dots,N)$$

- T : 温度
- R_{ij} : 熱抵抗
- C_i : 熱容量
- Q_i : 発熱量
- Q_{ij} : 熱流



証明証収集情報生成装置、証明証検証装置および公開鍵暗号運用システム 特許第3801782号(特開2000-10477)

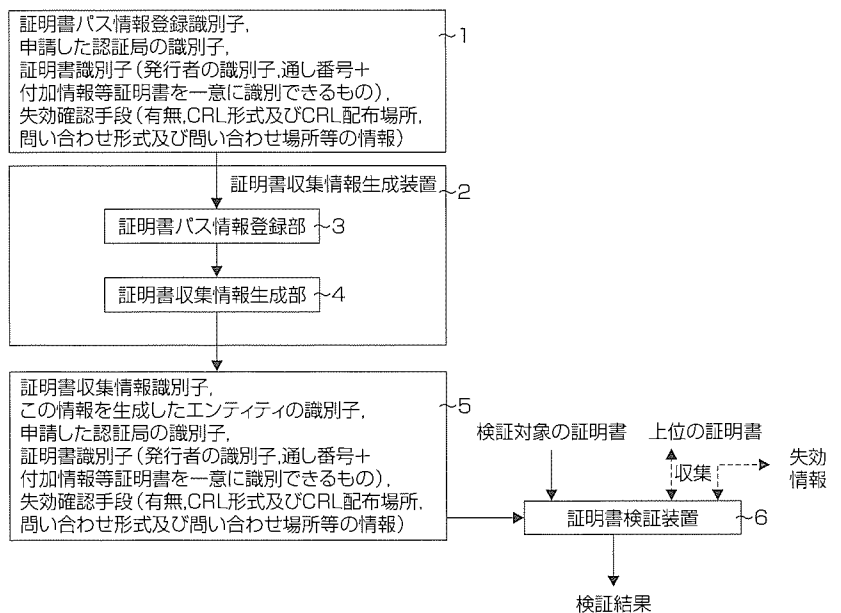
発明者 榊原裕之, 吉武 淳

この発明は、公開鍵暗号基盤の運用における証明書の検証処理の効率化に関するものである。

証明書の検証処理では、検証対象の証明書から検証者が信頼する証明書にたどり着く証明書のパスを構築した後、パスを逆方向に署名・失効のチェック等を行う。従来のパスの構築の処理では、証明書をデコードし、中に含まれる上位の証明書の識別子を調べ取得するという処理を繰り返すため、パスの構築に時間がかかるという課題があった。さらに、パス上の証明書の失効をチェックする失効情報も逐次収集するため、更に効率を低下させる原因となった。

装置(6)に入力することで、証明書の識別子のみからパスを決定可能となりパスの構築処理が低減される。さらに、失効情報の収集処理も低減される。

この発明では、証明書収集情報生成装置(2)を保持する機関が、認証局の申請に基づき、認証局の証明書を検証するために必要なパスと失効情報の識別子を証明書収集情報(5)として出力する。検証者は、検証する証明書と証明書収集情報(5)を証明書検証装





特許と新案 * * *

三菱電機は特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社 知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

データ変換装置 特許第3035358号(国際公開番号WO 090/-09705)

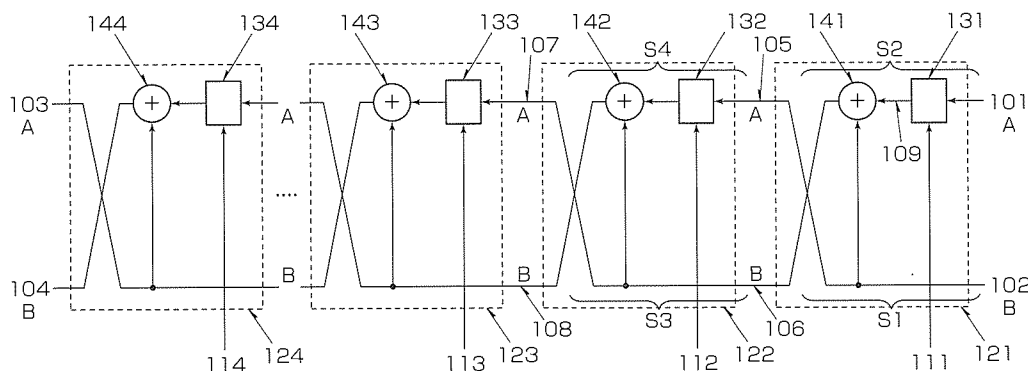
発明者 松井 充, 時田俊雄

この発明は、情報通信等においてデジタル情報を保護する入力データの暗号化と復号、及びデータ拡散等のためのデータ変換装置に関するものである。従来のデータ変換装置は、順次処理であるため処理が遅くなるという課題があった。

この発明は、上記の課題を解決するためになされたもので、複数の副変換処理を並列で行えるように構成して、暗号化・復号、及びデータ拡散等のデータ変換処理の高速化を目的とする。図はこの発明による暗号化回路である。この発明にかかわるデータ変換装置は、任意の二つのA入力データとB入力データに対し、二つの非線形変換(131,

132)と二つの鍵(かぎ)パラメータ(111, 112)を並列に作用させる機構を備え、その二組の変換結果の各々を二組の排他的論理和(141, 142)を介して次の段への入力とする構成をとっている。この構成を従属接続することで、奇数段相当の演算と偶数段相当の演算を並行して処理でき、演算の高速化を図ることができる。

この発明は、当社の暗号アルゴリズムMISTYや、第三代携帯電話W-CDMA方式の国際標準暗号であるKASUMIに使われている。また、この発明は、平成16年度全国発明表彰において恩賜発明賞を受賞した。



〈本号記載の商標について〉

本号に記載されている会社名、製品名はそれぞれの会社の商標又は登録商標である。

〈次号予定〉三菱電機技報 Vol.80 No.11 特集「FAシステム機器」/「家電機器」

三菱電機技報編集委員 委員長 三嶋 吉一 委員 小林智里 増田正幸 山木比呂志 佐野康之 中山保夫 世木逸雄 岡本尚郎 河合清司 長谷勝弘 木槻純一 逸見和久 光永一正 河内浩明 赤川正英 事務局 園田克己 本号取りまとめ委員 山田敬喜 福島康之	三菱電機技報 80巻10号 (無断転載・複製を禁ず) 編集人 三嶋 吉一 発行人 園田 克己 発行所 三菱電機エンジニアリング株式会社 e-ソリューション&サービス事業部 〒102-0073 東京都千代田区九段北一丁目13番5号 日本地所第一ビル 電話 (03) 3288局1847 印刷所 株式会社 三菱電機ドキュメンテクス 発売元 株式会社 オーム社 〒101-0054 東京都千代田区神田錦町三丁目1番地 電話 (03) 3233局0641 定 価 1部945円(本体900円) 送料別	2006年10月22日 印刷 2006年10月25日 発行
三菱電機技報 URL URL http://www.MitsubishiElectric.co.jp/giho/ 三菱電機技報に関するお問い合わせ先 URL http://www.MitsubishiElectric.co.jp/support/corporate/giho.html		
英文季刊誌「MITSUBISHI ELECTRIC ADVANCE」がご覧いただけます URL http://global.mitsubishielectric.com/company/r_and_d/advance/		

スポットライト

日本中央競馬会 東京競馬場納め 世界最大のオーロラビジョンLED

三菱電機は、2006年9月、日本中央競馬会東京競馬場向けに世界最大のオーロラビジョンを納入しました。

これまでも香港シャティン競馬場(世界最横長)、アトランタ・ブレイブスのターナー・フィールド(世界最大級)を納入してきましたが、今回のスクリーンは高さ11.2m、幅66.4m、面積にして743.68m²と今までのスクリーンを超える世界最大のスクリーンとなり、ギネスブックに認定されました。

このスクリーンはメインビデオスクリーン部と着順盤部が一体化していますが、運用上別々に制御する必要があるため、ビデオスクリーン用の連動する3台と着順用の独立した1台の計4台のコントローラで全スクリーンを制御します。

本場開催の際はメインビデオスクリーンと着順盤は独立していますが、イベント時には着順盤を含めたスクリーン全面での映像表示が可能となっています。

また、スクリーンの高い解像度を生かして複数のコンテンツを同時に放映することができます。このシステムは3人のオペレータがそれぞれのビデオ映像やオッズ等の表示内容を確認しながら(プレビュー機能)それぞれのスクリーンへの表示切換え(テイク機能)を独立してできるようになっています。これにより、複数の他場併売等の運用にも対応できます。

このスクリーンの表示コントローラは、従来の表示コントローラを発展させた新開発品で、複数のコントローラの同期運転による表示パターン制御の連動や全面ワイプ等が可能となっています。

さらに、ハイビジョン映像の1画面全面表示から最大4画面同時表示やハイビジョン映像上にデジタル映像を重ねて表示したり、半透明スーパーすることが可能となっており、ハイビジョン映像とデジタル映像を組み合わせた多彩

な表示パターンをレースの進行に合わせてタイムリーに切り換えて表示するなど最新機能を搭載しています。

スクリーン仕様

- ・縦11.2m、横66.4m
- ・絵素ピッチ 25mm(青1個、赤2個、緑1個)
- ・使用LED数 約476万個
- ・アスペクト比 9:53(縦:横)
- ・表示階調 4,096階調相当
- ・表示速度 60フレーム/秒
- ・輝度 5,000cd/m²

コントローラ仕様

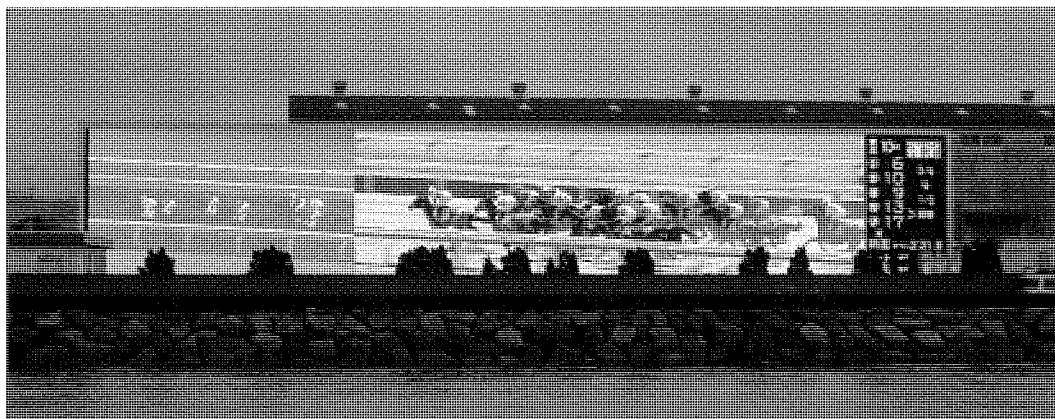
- ・映像入力信号
 - SD-SDI^(注1) (NTSC, PAL)
 - HD-SDI^(注2) (720p, 1080i)
 - DVI-D^(注3) (VGA^(注4), SVGA^(注4), XGA^(注4), SXGA, UXGA, 720p, 1080p)
- ・映像入力数
 - 4入力、任意位置での拡縮表示と表示順位の切換え可能
- ・高画質化処理
 - 動き適応型I-P変換 (NTSC, PAL, 1080i)
 - 色度変換(ナチュラルカラーマトリックス)
 - ダイナミックピクセル制御
 - 拡大時の鮮鋭度改善処理

(注1) SD-SDI : Standard Definition Television-Serial Digital Interfaceの略。

(注2) HD-SDI : High Definition Television-Serial Digital Interfaceの略。

(注3) DVI-D : Digital Visual Interface-Digitalの略。

(注4) VGA, XGA, SVGAは、米国IBM Corp.の登録商標です。



日本中央競馬会 東京競馬場納めオーロラビジョンLED

住所：〒100-8310 東京都千代田区丸の内2-7-3 (東京ビル)

会社名：三菱電機株式会社 お問い合わせ先：施設環境部 TEL 03-3218-4682