（独）科学技術振興機構（JST）
戦略的創造研究推進事業
チーム型研究CREST

# 実用化を目指した組込みシステム向け ディペンダブル・オペレーティングシステム

研究総括　所　眞理雄

（ソニー（株）コーポレートエグゼクティブSVP、

（株）ソニーコンピュータサイエンス研究所　代表取締役社長）

副研究総括　村岡　洋一

（早稲田大学　理工学術院　教授）

2007.5.7

# 戦略目標
# 高セキュリティ・高信頼性・高性能を実現する組込みシステム用の次世代基盤技術の創出

## 具体的な達成目標

（1）セキュアなオペレーティングシステム（OS）技術やコンパラ技術等のソフトウェア技術、超並列プロセッサアーキテクチャやシステムオンチップ(SoC)や再構成可能なハードウェア（リコンフィギャブル）技術等のハードウェア技術、高信頼リアルタイム保証技術、大規模システム構築化技術等、組込みシステムの次世代の基盤となる技術の研究開発を行い、**高セキュリティ・高信頼性・高性能な国産OSについて、実用化を視野に入れた開発を行う**。

（2）これらの技術開発により、**モバイル情報端末、車載機器、ウェアラブルコンピュータ等やそれらを応用した高性能コンピュータシステムの核となる組込みシステムにおいて、高セキュリティ・高信頼性を保ちつつ、高性能、リアルタイム性を保証することで、利用者が安心して高度なシステムやサービスを利用できるようになる**。

2007.5.7

# 戦略目標
# 高セキュリティ・高信頼性・高性能を実現する組込みシステム用の次世代基盤技術の創出

## 目標設定の背景及び社会経済上の要請

（1）モバイル情報端末、車載機器、ウェアラブルコンピュータ等の**我が国が得意とする組込みシステム**は、利用者のニーズに対して、高度な情報通信技術を活用することで、ユビキタスネットワーク社会における生活の利便性や快適性をもたらしている。 また、最近では組込みシステムの特性を活かし、高性能コンピューティング分野等の新しい分野への広がりをみせつつあり、ナノテクノロジーやライフサイエンスを始めとする科学技術や産業を革新し、国民や社会へ還元することがより一層期待されている。

（2）一方で、組込みシステムは、利用者の多種多様なニーズへ対応するためにシステムが複雑化、高度化しており、さらなる性能向上や高機能化を図るためには、個別システムごとの対応ではない基盤となるシステム構築技術が必要である。

（3）加えて、情報漏洩、ウィルス、不正アクセス、大規模システムダウンなどの利用者の安全・安心を脅かす諸問題が世界的規模で急激に顕在化・増大化しており、組込みシステムにおいてもこれらの問題に対する根本的な対応が必要かつ急務である。

2007.5.7

# 戦略目標
# 高セキュリティ・高信頼性・高性能を実現する組込みシステム用の次世代基盤技術の創出

## 目標設定の科学的裏付け

様々な脅威から情報を守るセキュリティ性とシステムに対する高信頼性を保証した上で、利用者が安心して組込みシステムを利用できるようにするためには、アクセス制御機能、高速・高信頼処理機能、高性能コンピューティング機能、高信頼システム構築機能、リアルタイム保証機能やソフトウェアバグからの保護機能の確保が必要になる。具体的には以下の技術開発・研究が必要である。

- アクセス制御機能
- 高速・高信頼処理機能
- 高性能コンピューティング機能
- 高信頼システム構築技術
  - コンパイラ技術、リソースアイソレーション、動的コンフィグレーション、高速リスタート、バーチャルマシン技術、ミドルウェア技術など
- リアルタイム保証機能
- ソフトウェアバグからの保護機能

# 研究領域
# 実用化を目指した組込みシステム向け
# ディペンダブル・オペレーティングシステム

**研究領域の概要**

コンピュータ技術の進展に伴い、基幹業務系や汎用PCのみならず、ホームサーバ、デジタルTV、組み込み型高性能サーバ、車載制御装置、生産制御装置、通信制御装置、ロボット、携帯機器、モバイル・ウェラブルコンピュータ、センサー・アクチュエータなど、多数の情報機器・システムがネットワークに接続されるようになってきており、近い将来にいわゆるユビキタス情報社会を構成するであろうと見込まれます。この時、これらの要素システムの多くは目的別の組込みシステムとして構築され、高い信頼性、応答性を確保しつつ、小さく、軽く実現することを要求されます。加えて、それらを接続した情報システムの信頼性、安全性、セキュリティー、性能などの要求を満足でき、さらには将来の拡張性や変更に動的に対応できなければなりません。このようなディペンダブルなシステムを構築するためには、オペレーティング・システム（OS）のレベルからイノベーティブな研究開発を行う必要があると考えられます。本研究領域は、ディペンダブルな情報システムを構築するための組込みシステム向けのOSの研究開発を行うものです。

領域では、将来、社会で実際に広範に使用されうるOS技術を創出するために、実用化を目指し、個別の研究成果を統合して実用システムとして実現が可能であることを実証し、オープンソースの形で将来の更なる研究開発の基盤を提供することを目指します。このため、本研究領域においては、研究総括の強い統率の下で、必要に応じて研究体制の再編や研究の進め方の調整を行うことにより、研究領域内の研究を横断・統合した推進体制をとり、適切な研究領域運営を行うこととします。

2007.5.7

# 研究総括の募集・選考・研究領域運営に当たっての方針

## （1）研究開発の範囲

- 本研究では、ディペンダブルOSを大枠として以下のような機能を持つものと定義します。①処理要求（負荷）の変動に対して、必要な応答性・リアルタイム性を保持する。②個別のハードウエア、ソフトウエア、通信システムの故障や障害に対して、情報システム全体を停止させない。③ネットワークを介した過失や故意の攻撃に対してシステムの性能を確保する。④ソフトウエアの変更・改良が情報システム全体を停止させることなく安全に行える。⑤これらにより、情報システム全体が致命的な状態に至ることなく、安全、快適に利用できる。

- このような組込みシステム向けディペンダブルOSを実現する具体的な技術としては、高信頼実時間制御技術、高信頼通信制御技術、アクセス制御技術、高信頼ファイルシステム技術、ハードウエアセキュリティーモジュールを用いた高信頼実行技術、仮想マシン技術、故障隔離技術、再構成技術，高速再起動技術、高性能マルチコア管理技術、組み込み型高性能並列処理技術、高可用性技術、高信頼ソフトウエア構築技術、などが含まれると考えますが、これに限定するものではありません。

# 研究総括の募集・選考・研究領域運営に当たっての方針

（2） 募集・選考に当たっての方針

- ここで研究開発されたディペンダブルOSは、要素技術としては3年から5年の内に、また、大きなまとまりとしても10年以内に実用に供され、広く世界で使用されるとともに、オープンソースの形で将来の更なる研究開発の基盤を提供することを目指します。従って、利用者や将来の研究開発者が受け入れやすい形で開発することが大切になります。そのためには、オープンソースのOSをベースとして研究開発を行うことが有効な方法であると考えます。ただし、そのような進め方においても、革新的な要素を含みイノベーションに貢献する技術を生み出す研究開発の提案であることが必須です。

- 本研究の成果が実用システムとして利用可能なことを実証して行くためには、個別の研究成果を統合し、実際に応用システムを構築することが必須となります。このためには研究チーム間の連携のみならず、応用システムを持つ企業との共同研究推進体制の構築や国内外の普及促進団体との連携など、単なる研究を超えた実用化ならびに普及促進のためのあらゆる方策を実施することも必要になります。

- 平成19年度は、18年度の検討ならびに基本アーキテクチャの設計を拡充し、組込みシステム向けディペンダブルOSの機能の充実ならびに実用性の向上のための研究課題の提案を歓迎します。とりわけ、耐攻撃性の向上のための高信頼通信制御技術やアクセス制御技術、高信頼ファイルシステム技術、故障解析技術、ハードウェアセキュリティーモジュールに関連する技術などが18年度採択課題を補強する上で重要であると考えております。重ねて、19年度新規採択課題は18年度採択課題と独立のものではなく、一体として統一的な最終目標に向かって研究開発を進めるものであることを理解したうえ、研究課題を提案してください。

2007.5.7

# 研究総括の募集・選考・研究領域運営に当たっての方針

（3）期待される成果

アルゴリズムや計算モデルなどの基盤研究の論文発表に留まることなく、実際にシステムを構築するなどによって、その実用可能性を実証することが必要です。すなわち、論文のみならず、実用可能性を実証できる形で実現したソフトウエア自身を研究成果と考えます。更には、各研究チームはそれぞれ個別の成果のデモを行うとともに、研究チーム間の協力の下に統合システムとしてのデモを行うこととし、統合されたソフトウエア自身を本研究領域の最終的な研究成果と考えます。

# 研究総括の募集・選考・研究領域運営に当たっての方針

（4）運営に当たっての方針（その1）

- 本研究領域では、実用化と将来の更なる研究開発の基盤を与えることを目標とするため、各研究課題の研究成果を統合し、全体システムとして実用に近い形でデモを行い、その有効性ならびに実用性を実証します。このため、研究の初年度には、研究総括ならびに領域アドバイザーのもとに平成18年度採択の研究チームを含め、研究チーム相互の頻繁な議論を行い、全体システム像を明確にし、個々の研究課題の研究開発テーマを再定義し、研究ならびに開発設計を行ってゆくことになります。従いまして、この段階で研究計画の大幅な変更をお願いする場合があります。

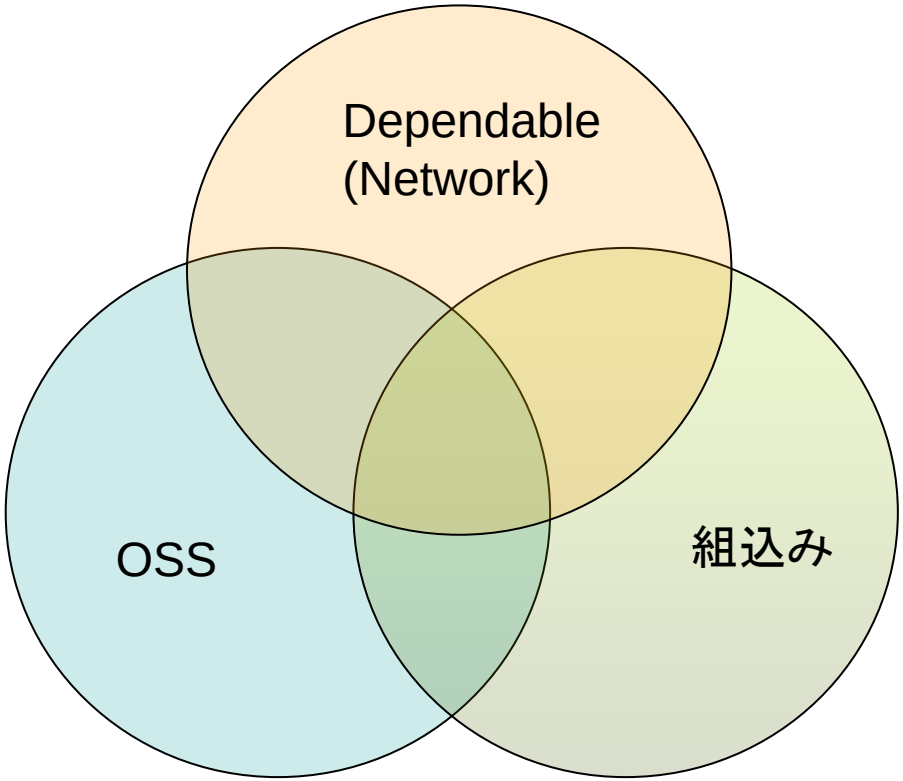
- 平成18年度採択のテーマとあわせて統合のデモならびに最終評価を行うことを目的とし、平成19年度採択のテーマの最終年度は平成23年度（2012年3月終了）とします。それぞれの研究チームは初年度中に再定義された研究計画をもとに、第3年度終了までに成果のデモを行い、その結果によって、研究の継続、変更、中止が判断されます。研究の継続や変更が判断された研究課題は、研究の最終年度における全体システムの再定義、最終年度におけるデモの設計などについて研究統括ならびに領域アドバイザーのもとに議論を行い、最終年度に向けての個々の研究課題の研究計画を再定義し、精緻化し、その後研究開発を進めます。

# 研究総括の募集・選考・研究領域運営に当たっての方針

（4）運営に当たっての方針（その2）

- 研究チーム間の緊密な連絡を可能にし、共同作業を効率よく進め、研究開発者・技術者を集結し、あるいはリソースを共用し、想定される利用者等との情報交換を行い、最終的な研究成果物をより有益なものにするために本研究領域では平成19年4月より研究センター機能を設置することといたしました。研究センターには研究センター長を置き、また、若干名の研究要員、開発要員を置き、研究開発の一部を研究チームとの連携の下に行い、研究成果を統合し、最終デモを各研究チームと一体になって行います。また、研究成果の広報ならびに利用推進を図ります。研究計画書作成に当たっては、研究センターの有効利用に付いてもご検討下さい。

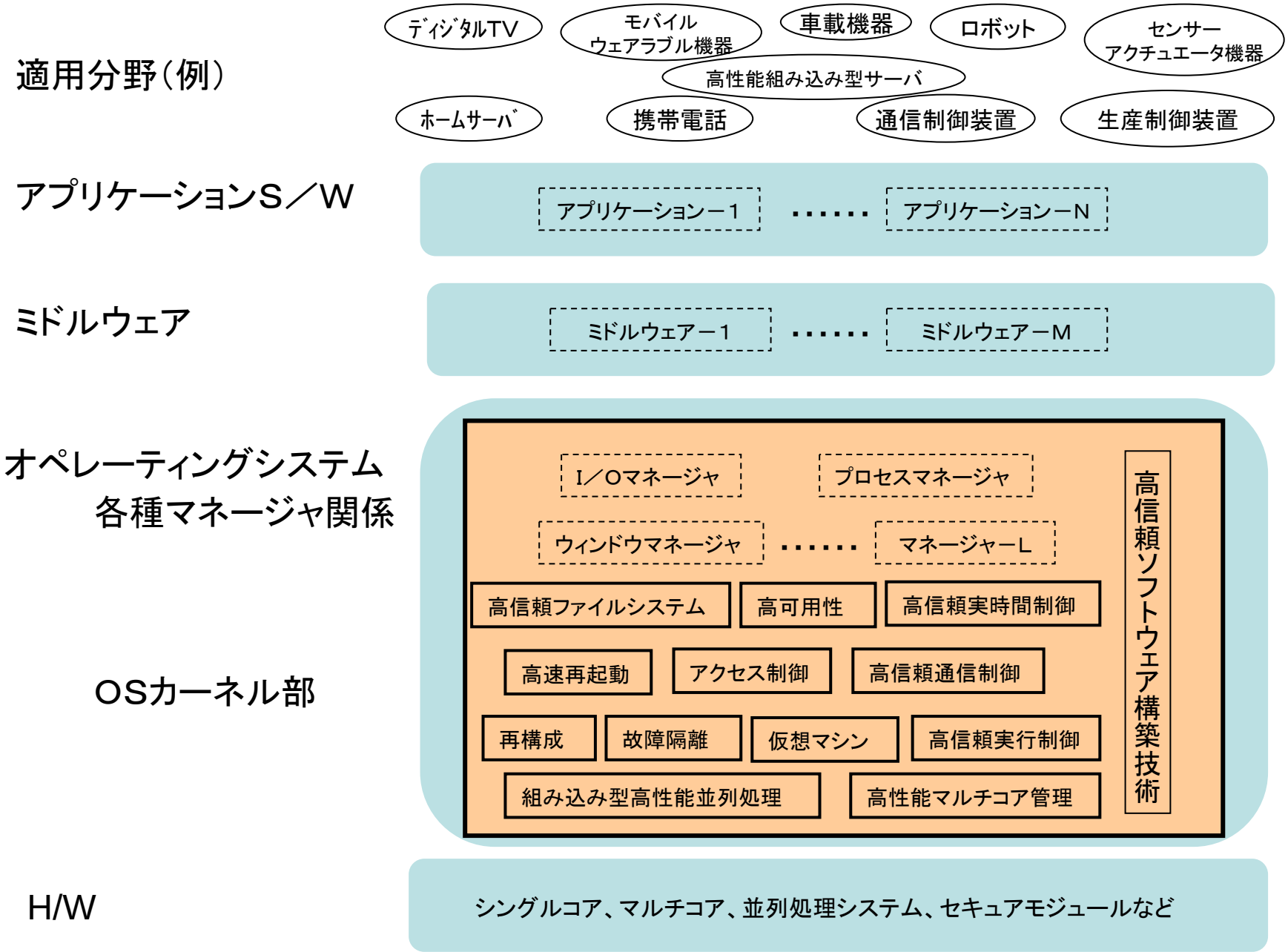
# 研究開発領域




1. 処理要求（負荷）の変動に対して必要な応答性・リアルタイム性を保持
2. 個別のハードウェア、ソフトウエア、通信システムの故障や障害に対して情報システム全体を停止させない
3. ネットワークを介した過失や故意の攻撃に対してシステムの性能を確保する。
4. ソフトウエアの変更・改良が情報システム全体を停止させることなく安全に行える。
5. これらにより、情報システム全体が致命的な状態に至ることなく安全、快適に利用できる

# 目的と成果目標

- 目的（1）（直近）
  - ホームサーバー、デジタルTV、組み込み型高性能サーバー、車載制御装置、生産制御装置、通信制御装置、ロボット、携帯機器、モバイル・ウェラブルコンピュータ、センサー・アクチュエータ、などを対象
  - 応答性、リアルタイム性
  - 高信頼性
  - 高アベイラビリティー
  - 高ネットワーク・セキュリティー
- 目的（2）（長期的目的）
  - 全ての機能がネットワークでつながれた社会のロバストネスを確保する
- 成果目標
  - 実用システムとして実現（実装）し、製品に使ってもらう
  - 次世代システムの開発の基盤として利用されうる
  - オープンソースコミュニティーに貢献


適用分野（例）
ディジタルTV
モバイル
ウェアラブル機器
車載機器
ロボット
センサー
アクチュエータ機器
高性能組み込み型サーバ
ホームサーバ
携帯電話
通信制御装置
生産制御装置
アプリケーションS／W
アプリケーション－1
アプリケーション－N
ミドルウェア
ミドルウェア－1
ミドルウェア－M
オペレーティングシステム
各種マネージャ関係
I／Oマネージャ
プロセスマネージャ
ウィンドウマネージャ
マネージャ－L
OSカーネル部
高信頼ファイルシステム
高可用性
高信頼実時間制御
高速再起動
アクセス制御
高信頼通信制御
再構成
故障隔離
仮想マシン
高信頼実行制御
組み込み型高性能並列処理
高性能マルチコア管理
高信頼ソフトウェア構築技術
H/W
シングルコア、マルチコア、並列処理システム、セキュアモジュールなど
2007.5.7
：ディペンダブルOS
：今回の主な開発課題
：検証時に必要になるS／W

# 方法

- オープンソース （e.g., Linux） をベースにディペンダビリティー機能を強化
- 実用化を目標、普及を推進
- 大学＆企業の共同体制の確立
  - ばらばらにやっても実用に供するものは出来ない。基本的には組織化して進める。
  - 全体のシステム設計の中に、応用別（センサーネット、ロボット、ケータイ、CE、HDD付き・無し、メモリー３２MB以上・以下など)のプロジェクトを含むことは良い。ネットワーク機能は必須とする

# センター機能（1）

- なぜ必要か？
  - 組み込みOSの特徴
    - 多様なハードウエアプラットフォーム
    - 多様な要求
    - 多様なデバイスドライバー
    - 企業との連携の重要性
  - 実装・実用化が主眼
- 何をやるか？
  - 研究チーム間の共同作業の効率的実行
  - 利用者との情報交換や共同作業の場の提供
  - オープンソースコミュニティーとの連携の要員
  - 研究成果の統合、デモの推進
  - 研究成果の広報、利用促進

# センター機能（２）

- センターの運営に関連した方針
  - 研究センターには、前述の機能を果たすために、研究センターに研究者・技術者を置き、また研究のコーディネーション、情報収集、広報、などの若干の事務員を置く。
  - 研究センターでは、各研究チームでの研究を統合するための研究開発や、全体システムの構築に必要であるが、研究チームの研究開発だけではカバーされないような研究開発も行う。また、研究チームの研究開発の一部を共同で行うことも考えている。
  - また、実用性の実証のためのシステム構築は、該当するアプリケーションを持つ企業と協力することによって新たな開発による二重投資を極力避ける。
  - このため、各研究チームは、ソフトウエア開発の外注を出来る限り避け、オンサイトで一緒に研究開発が出来るような研究チーム作りを行う。

# 関連団体等

- Open Innovationを志向
  - CELF
  - TCG
  - OSDL
  - 日本OSS推進フォーラム
  - IPA　OSSセンター
  - その他

# 研究開発の成果公開の範囲

- Linuxをベースとした場合
  - GPLの範囲についてはソースコードを公開
  - ミドルウエアやアプリケーションについてのソースコードの公開非公開は任意
  - コンソーシャム化する場合は（ミドルウエアやアプリケーションのソースは）RANDか？ （Reasonable and Non-Discretionary)
- その他の場合は個別検討

# 運営と評価

- 密接な連携
  - 研究会、ワークショップ、講演会、コードレビューなど頻繁に開く（毎週？）
  - 企業（利用者）からも連携研究員として参加していただきたい
  - センターの利用（継続検討課題）
- 評価
  - 実用性と新規性評価
  - 特許
  - 論文
  - 個人によるコミュニティー貢献がベース
- 領域アドバイザー
  - 応募選考、アドバイス、中間・最終評価、を行う
  - 大学関係3名、企業関係3名
- 領域運営アドバイザー
  - 領域の運営方針や研究推進に関する助言・協力
  - 成果発表・成果普及などに関する助言・協力
  - 大学関係3名、企業関係4名
- 研究推進委員
  - 実質的に研究開発に貢献
  - 企業関係6名

# プロジェクトメンバー

【研究総括】

| | |
|---|---|
| 所　眞理雄 | ソニー株式会社　コーポレート・エグゼクティブSVP<br>株式会社ソニーコンピュータサイエンス研究所　代表取締役社長 |

【副研究総括】

| | |
|---|---|
| 村岡　洋一 | 早稲田大学　理工学部　教授 |

【領域アドバイザー】（07/4/1現在）

| | |
|---|---|
| 岩野　和生 | 日本アイ・ビー・エム株式会社　ソフトウェア開発研究所　執行役員・所長 |
| 妹尾　義樹 | 日本電気株式会社　インターネットシステム研究所　統括マネージャ |
| 田中　英彦 | 情報セキュリティ大学院大学　情報セキュリティ研究科　研究科長・教授 |
| 西尾　章治郎 | 大阪大学 大学院情報科学研究科　研究科長・教授 |
| 松田　晃一 | NTT-AT IPシェアリング株式会社　代表取締役社長 |
| 安浦　寛人 | 九州大学　大学院システム情報科学研究科　教授<br>システムLSI研究センター　センター長 |

2007.5.7

【領域運営アドバイザー】（07/4/1現在）

| | |
|---|---|
| 勝丸　泰志 | 富士ゼロックス株式会社　オフィスプロダクト事業本部　副本部長 |
| 鎌田　富久 | 株式会社ACCESS　取締役副社長兼CTO |
| 菊野　亨 | 大阪大学大学院情報科学研究科　教授 |
| 櫛木　好明 | パナソニックモバイルコミュニケーション株式会社　代表取締役社長 |
| 鶴保　征城 | IPA　ソフトウェア・エンジニアリング・センター（SEC）　所長 |
| 田中　譲 | 北海道大学大学院情報科学研究科　教授 |
| 丸山　好一 | 日本電気株式会社　執行役員常務 |

【研究推進委員】（07/4/1現在）

| | |
|---|---|
| 浅井　信宏 | 日本アイ・ビー・エム株式会社　ソフトウェア開発研究所<br>WPLC & パーベイシブ・ソリューション開発　部長 |
| 上田　理 | ソニー株式会社　技術開発本部　SS開発部　テクニカルマネージャー |
| 柴田　次一 | 日本電気株式会社　コンピュータソフトウェア事業本部 OSS推進センター　グループマネジャー |
| 高澤　真治 | 日本SGI株式会社　エンタープライズLinuxソリューションセンター チーフLinuxコンサルタント |
| 山浦　一郎 | 富士ゼロックス株式会社 オフィスプロダクト事業本部<br>コントローラプラットフォーム開発部　グループ長 |
| 横山　和俊 | NTTデータ　技術開発本部　ソフトウェア工学推進センター シニアスペシャリスト |

2007.5.7

【センター長】（07/6/5着任）

| | |
|---|---|
| 屋代　眞 | 現職:　日本アイ･ビー･エム株式会社　理事<br>開発製造　R&D イノベーション･サービス　企画担当 |

【研究代表者】

| | |
|---|---|
| 石川　裕 | 東京大学　情報基盤センター　教授 |
| 高信頼組込シングルシステムイメージOS | |

| | |
|---|---|
| 佐藤　三久 | 筑波大学　大学院システム情報工学研究科　教授 |
| 省電力高信頼組込み並列プラットフォーム | |

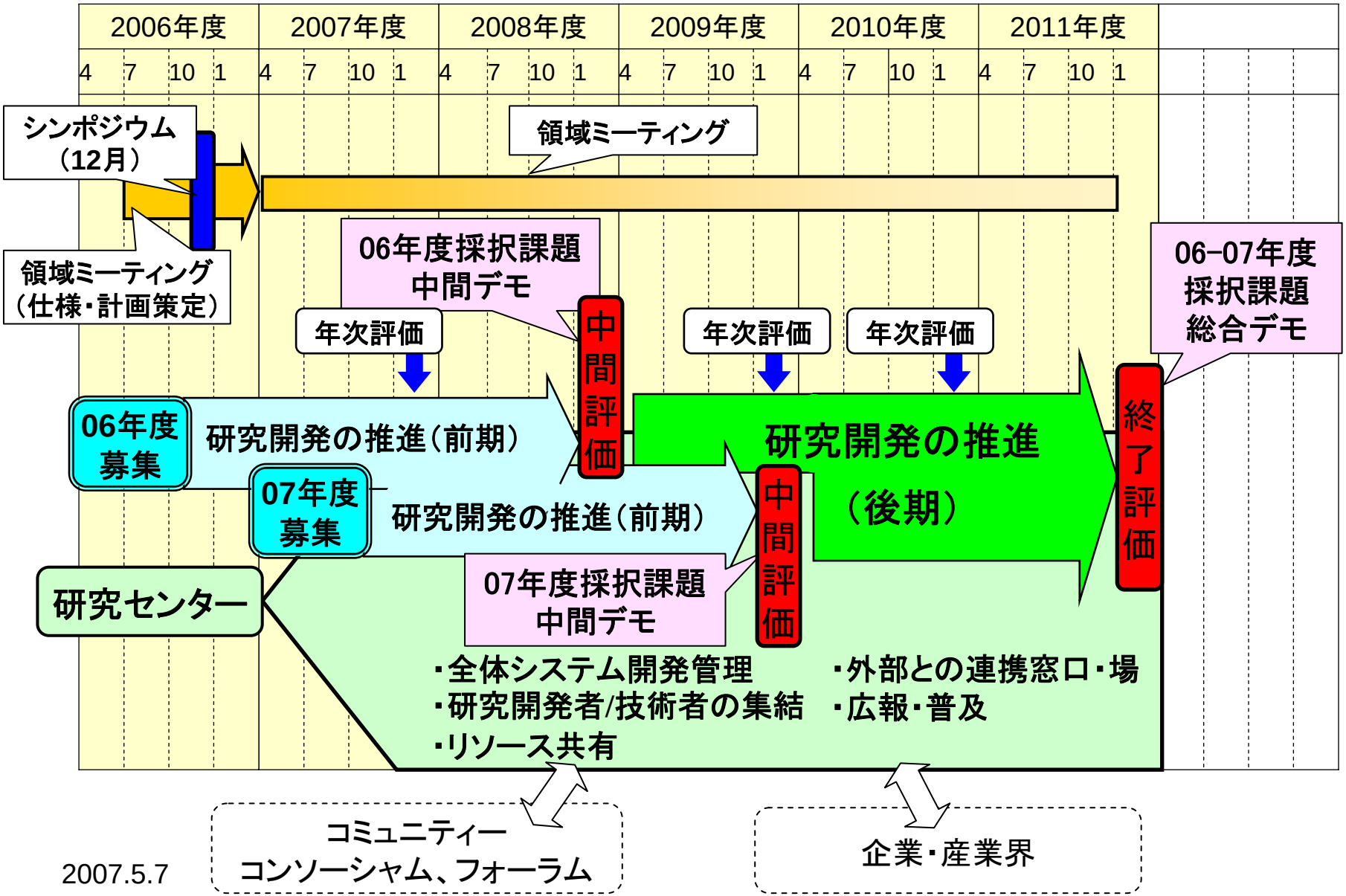
| | |
|---|---|
| 徳田　英幸 | 慶應義塾大学　環境情報学部　教授 |
| マイクロユビキタスノード用高信頼OS | |

| | |
|---|---|
| 中島　達夫 | 早稲田大学　理工学術院　教授 |
| 超高機能情報家電のためのオペレーティングシステム | |

| | |
|---|---|
| 前田 俊行 | 東京大学　大学院情報理工学系研究科　助手 |
| 高信頼システムソフトウェア構築技術に関する研究 | |

2007.5.7

# 研究開発スケジュール




2007.5.7

# まとめ

- 真の産学協同プロジェクトとして絶対に成功させる
- 実用的なソフトウエア開発プロジェクトとして絶対に成功させる
- 将来の開発のための基盤として使ってもらえるようにする
- 以上をもとに、全てがネットワークに依存した次世代社会のインフラストラクチャーとして必須であるディペンダブルOS（通信プロトコルを含む）を開発し、オープンソースとして人類社会に貢献する