# ロバストな組み込み向けオペレーティングシステム

## １．背景

我々の生活は,マイクロプロセッサの組み込まれた機器，そして世界中を網羅するネットワークの普及によって大きな変化を迎えようとしている．これらのユビキタスコンピューティング環境は今後より一層整っていくものとみられる．同時に，家電や機器に埋め込まれている組み込みシステムの複雑さは増大すると予測される．このような環境下では，組み込まれたコンピュータ，ネットワークを保護しながら有効に活用するため，より強固なシステムを開発してゆく必要がある．そこで我々は，組み込みシステムのためのロバストネスを向上するための機能の開発を行う．

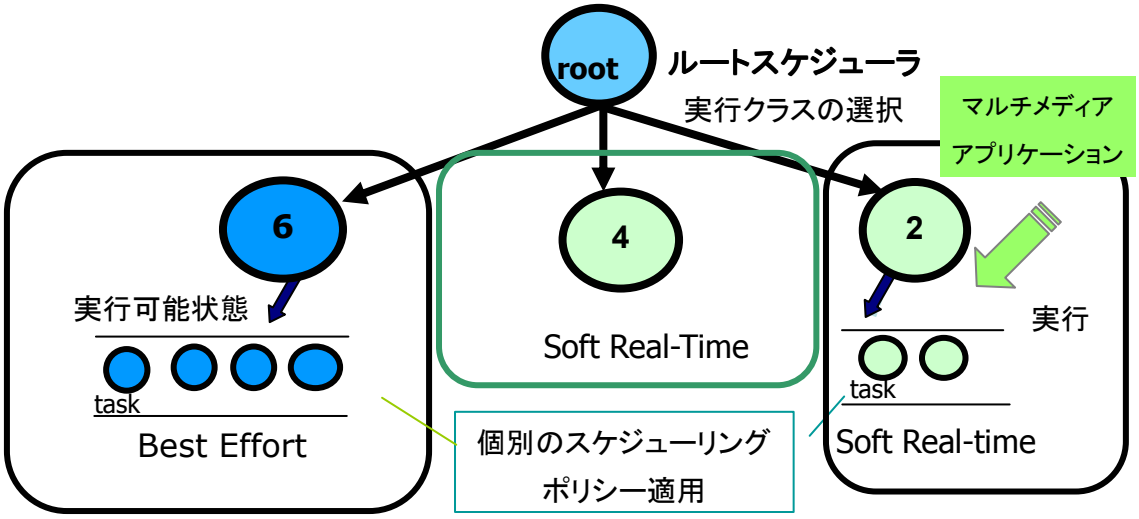
## ２．目的

組み込みシステムでは，アプリケーションに割当てられる資源量が正しく制御されない場合には，システムの振る舞いが異常を起こすと，それがそのまま我々の生活に支障を生じさせてしまう可能性がある．特に，ネットワークに接続された場合，外部からの攻撃によってリソースが不適切に使用されてしまう可能性があり，危険性は増大する．このような不具合を生じさせないロバストなシステムを構築するために，各アプリケーションが使用する資源の管理機能により，資源を間違って使用してもシステム全体の振る舞いに異常を生じないようにする．アプリケーションが動的に追加される可能性のある将来の組み込みシステムでは，重要な機能となる．

信頼性を高めることは，またロバストなシステムを構築するためには重要である．信頼性を高める一つの方法として，システムが自身の障害を検知し，それを自動的に回復する機能を開発する．組込みシステムにおいては，メインフレームで実現されているようなハードウェアによる信頼性を高めるための障害検知および回復機能は使用することができない．そこで，仮想オペレーティングシステムアーキテクチャを用いてソフトウェア的に冗長性を高めたソフトウェアアーキテクチャを，組込みシステムのための障害検知および回復機能として開発する．また，障害検地のための仮想オペレーティングシステムアーキテクチャを用いた場合でも，アプリケーションに割当てられる資源量を正しく制御するための，資源管理を可能にする機能として階層的資源管理機能の開発を行う．

## ３．開発の内容

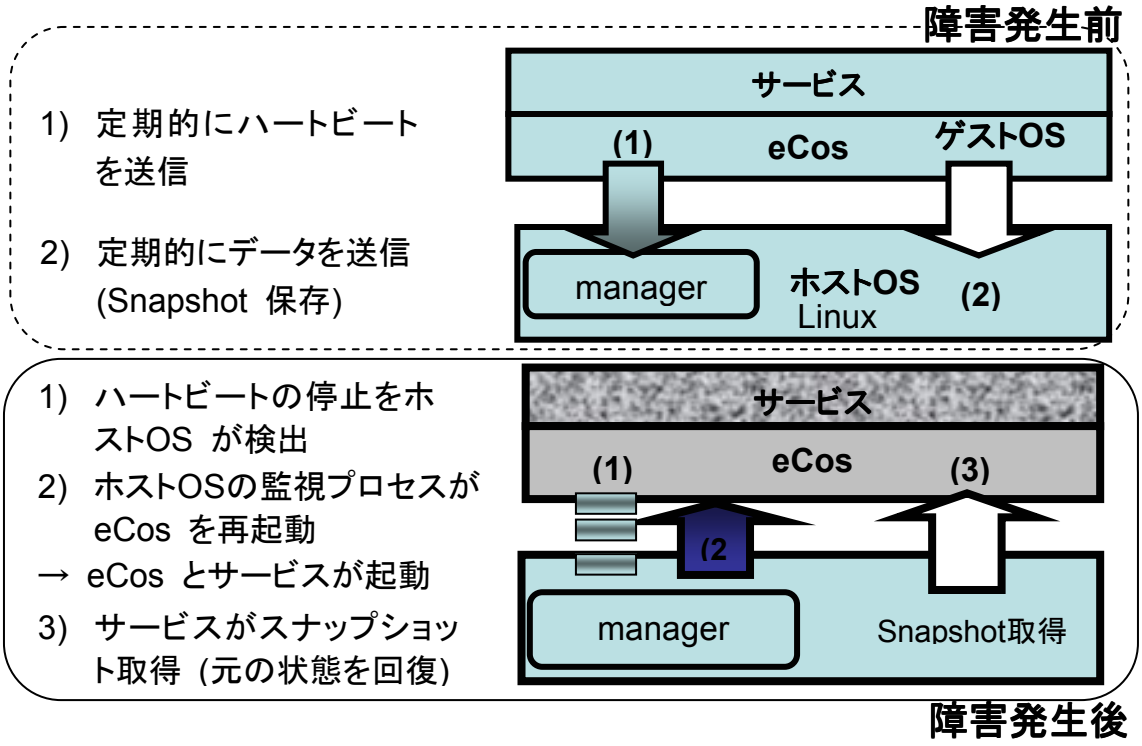
本プロジェクトで開発するロバストな組込み向けオペレーティングシステムは，資源管理機能，階層的資源管理機能，障害回復機能からなる．
資源管理機能では，クラス別スケジューラをベースとした多様なアプリケーションに適合した管理方式を提案する．スケジューラはプロポーショナルシェアアルゴリズムによる重みづけに基づいた公平スケジューリングを実現する．管理ドメインをクラスという形で分ける事により，クラス相互の独立性が高まるためセキュリティの観点からも望ましい．さらにアドミッション機能を組み合わせる事により，アンセキュアなプログラムが実行される際，そのプログラムの資源利用に対して制限をかけるための判断及びキャップを行う．この技術を組み合わせることで、ロバストな OS としての資源管理機能が可能となる．




階層的資源管理機能では，OS が仮想化され階層的に構成された場合の資源予約をサポートする．OS 仮想化技術は，一つのコンピュータ上で複数の仮想 OS を稼動させる技術である．OS 仮想化技術を組込みシステムに応用することにより，ユビキタスコンピューティング環境が商用化された場合などに必要となる高いセキュリティが提供可能である．OS 仮想化技術により複数の仮想 OS を同時に単一コンピュータ上で動作させることで，仮想的に独立した実行環境を提供できる．即ち，各ユーザの実行環境を別の仮想 OS 上に作ることで，それぞれの実行環境を分離することが可能になる．また，資源管理面でのセキュリティ向上のために，階層的資源管理機能では，仮想 OS における資源管理機能を提供する．

障害回復機能では，OS に障害が発生した際にアプリケーションと連動して障害復旧を行う新しいフレームワークを提示する．我々の提示する新しいフレーム

ワークではOS仮想化技術を用いることで従来OSとして動いていた部分とハードウェアとの間に仮想化レイヤを挿入し，仮想化レイヤ上のアプリケーションからOS部分の実行を監視する．この機能によって，実行中のOSに致命的な障害が発生してシステムが停止した場合でも，ソフトウェア的に再起動が可能である．また，このフレームワークではOS上で動いているアプリケーションのデータのバックアップを仮想化レイヤ上に保存する仕組みも兼ね備えている．




## ４．従来の技術との相違

資源管理機能では，多様なアプリケーションに適合可能なクラス別スケジューラによる資源管理を行う．管理ドメインをクラスという形で分け，それらをプロポーショナルシェアアルゴリズムによる重みづけに基づき資源割り当てを行うことにより，クラス相互の独立性が高め資源管理の面のセキュリティを向上させる．さらにアドミッション機能を組み合わせる事により，アンセキュアなプログラムに対するプロテクションを向上させる．階層的資源管理機能では，高いセキュリティを提供するために OS 仮想化技術を組込みシステムに応用した場合での，資源予約をサポートする．OS仮想化技術により複数の仮想OSを同時に単一コンピュータ上で動作させることで，仮想的に独立した実行環境を提供できるため，セキュリティ上問題があるかどうかわからないプログラムの実行ために別の仮想OSを用意することにより，被害を最小限に抑えることができる．障害回復機能では，同じくOS仮想化技術を用いて，OSに障害が発生し

た際にアプリケーションと連動して障害復旧を行う機能を提供する．仮想 OS を用いることにより，仮想 OS は仮想化レイヤからの監視が可能になる．それにより，仮想 OS での障害発生時にそれを検知して自動的に再起動が可能になる．また，アプリケーションスナップショット機能により，プログラム実行の継続をサポート可能である．

## ５．期待される効果

**セキュリティの強化：**本システムは CPU，メモリといった各プロセスのリソースを制御することにより仮想的にセキュアな環境を設ける．これにより，資源管理面でのセキュリティを強化することができる．

**Linux 利用の促進：**本システムでは，ベースを Linux としている．現在 Linux はフリーのオペレーティングシステムとして誰もがソースコードを利用できる GPL のライセンス形態をとっている．オープンなシステムを利用することで，次世代に研究資産が継承され，継続的に研究開発活動が充実してゆくことを促進する．

**組み込み分野：**日本の組み込み分野でのプレステージは，品質のよいチップとオペレーティングシステムによって支えられている．これからの組み込みシステムがさらに複雑化するなかで，本研究は安定した実行環境を提供するメカニズムを提供するものである．

## ６．普及（または活用）の身通し

本研究の成果は国内，国外学会での論文発表により成果を広く知らしめ，また開発プログラムについては配布のためのウェブページを作成する予定である．

## ７．開発者名（所属，e-mail アドレス）


- 追川修一（早稲田大学大学院理工学研究科，shui@dcl.info.waseda.ac.jp）
- 菅谷みどり（早稲田大学大学院理工学研究科，doly@dcl.info.waseda.ac.jp）
- 岩崎匡寿（早稲田大学大学院理工学研究科，pingoo@dcl.info.waseda.ac.jp）
- 鈴木裕介（早稲田大学大学院理工学研究科，suzuyu@dcl.info.waseda.ac.jp）
- 松浦杏子（早稲田大学大学院理工学研究科，kyo@dcl.info.waseda.ac.jp）
- 小林宣幸（早稲田大学大学院理工学研究科，koba-n@dcl.info.waseda.ac.jp）