

# QNX Neutrino RTOS セキュア カーネル

コモンライテリア認証、最大の信頼性を提供するメモリ保護マイクロカーネル アーキテクチャ、比類のないスケラビリティ、リアルタイム パフォーマンス

QNX®のリアルタイムOS技術は、1980年から、多くのメーカーにより、安全性が不可欠なアプリケーションで使用されてきました。医療機器、緊急応答センター、軍事通信、原子力モニタリング、インターネットルーター、車載インフォテイメントシステムなど、採用分野は多岐に渡ります。これらのQNX搭載システムは、規模の大小や複雑さのレベルに関わらず、一日24時間、一年365日ノンストップで稼働できる比類のない信頼性とセキュリティで知られています。

## マルチコア処理の活用

QNX Neutrino® RTOS セキュア カーネルは、コモンライテリア認証を取得したフル機能RTOSであるだけでなく、マルチコアプロセッサ用に対称型マルチプロセッシング (SMP) と限定型マルチプロセッシング (BMP) を実装している唯一のコモンライテリア認証済みRTOSです。このため、QNX Neutrinoは、優れたマルチコア設計に必要となる並行処理機能に対応する唯一の認証済みRTOSということになります。

## セキュアなシステムの構築

QNX Neutrinoのユニークなアダプティブパーティショニング技術は、アプリケーションにシステムリソースを確保し、同時に、不良ソフトウェアがシステム内のほかのコンポーネントからリソースを完全に奪ってしまうことを防ぎます。システムがオーバーロード状態になると、アダプティブパーティショニングはリソース確保を実行し、アプリケーションが割り当てられたリソースバジェットを確実に取得できるようにします。

## セキュアな設計のマイクロカーネル



マイクロカーネル RTOS は、プロセスとプロセスの間に保護バリアを提供します。こうしたプロセスの中には、通常モノリシック オペレーティング システムではカーネルスペース内のあるネットワークやファイルシステムも含まれます。

## 耐障害性の高いアプリケーションの構築

市場において長きに渡る稼働実績を誇るQNX Neutrino RTOS は、真のマイクロカーネル アーキテクチャに基づいています。このOSでは、すべてのドライバ、アプリケーション、プロトコルスタック、ファイルシステムが、カーネルの外側にあるメモリ保護されたユーザースペースで実行されます。事実上、どのコンポーネントに障害が発生しても、自動的な再起動が可能であり、ほかのコンポーネントやカーネルに悪影響が及ぶことはありません。さらに、QNX Neutrinoには、ハイアベイラビリティフレームワークのオプションがあるため、クリティカルなソフトウェアを監視し、障害発生後も実行を継続することができます。ここまですべての障害回避と回復を提供できる商用RTOSは、ほかには存在していません。

構造的にモジュール仕様になっているQNX Neutrinoでは、システム稼働中にモジュールのアップデートや新機能の導入、バグ修正の適用などが可能であり、コストを発生させるダウンタイムやシステム停止は不要です。

## セキュアなプログラミング規格

POSIX 規格 (1003.1 – 2000 PSIX.1) に従って開発されたQNX Neutrino RTOS は、よく知られたプログラミングAPIと、セキュアシステムで非常に重要となる「予測可能で安定した動作」を提供します。このPOSIX APIは、安全ではない動作や誤解される結果の可能性を含んだプロプライエタリインターフェイスの使用を

防ぎます。しかも、POSIXでは、ユーザーおよびグループ権限があり、必要であれば、高い権限に対してもシステム リソースへのアクセスを拒否するセキュリティ デフォルト機能を正確に守ることが要求されます。また、POSIX プログラミングの使用には、レガシー コードやオープン ソースのUNIX、Linux、インターネットのコードを、シンプルな再コンパイルのみでポータリングできるという利点があります。開発者に馴染み深い標準 API により、アプリケーション コードを再使用して、作業の遅れによるコストの発生を防ぎ、開発サイクルをスピードアップして製品の市場投入までにかかる時間を短縮することができます。

## 開発プロジェクトのスケールングに対応

QNX Neutrino が提供する根本的なマルチコア対応機能とビルトイン透過分散処理を活用し、耐障害性に優れたスケールの大きなシステムを構築することができます。設計要件に関わらず、開発者は同じ RTOS、ツール、API、ソースコードをすべてのプロジェクトで使用することができます。その結果、より寿命の長い製品、開発時間の短縮、投資からの大きなリターンを実現することができます。

## Foundry27

QNX ソフトウェア開発者のコミュニティ ポータルである Foundry27 では、ソース レポジトリ、フォーラム、ブログ、wiki などをホストしています。アイデアの討論、QNX コミュニティの新しいコード プロジェクトなど、開発者のさまざまな目的にあわせたリソースを Foundry27 は提供します。

## QNX ソフトウェア システムについて

Research In Motion Limited (RIM) の子会社である QNX ソフトウェア システムズは、組込み市場を対象としたミドルウェア、開発ツール、オペレーティング システム ソフトウェア、プロフェッショナル サービスなどにおけるリーダーです。シスコ、ダイムラー、ゼネラル エレクトリック、ロッキード マーティン、シーメンスといった、世界のリーダー企業が、車載テレマティクスユニット、ネットワーク ルーター、産業制御システム、医療機器、軍事防衛システムなど、安全性が不可欠となるミッションクリティカルなアプリケーションで QNX の技術を採用しています。



QNX SOFTWARE SYSTEMS

## QNX Neutrino RTOS セキュア カーネル

### コモンクライアント (ISO/IEC 15408) EAL+ 認証

- ▶ 開発プロセスとセキュリティに対する厳しいスタンダード
- ▶ 初のEAL+認証フル機能 RTOS
- ▶ 規格認証にマルチコア プロセッサ用 SMPサポートとアダプティブパーティショニング技術を含めた初の RTOS

### マイクロカーネル アーキテクチャ

- ▶ ダイナミックにアップグレード可能なサービスとアプリケーション
- ▶ 緻密な障害隔離と回復
- ▶ メッセージ バッシングにより明確に定義されたモジュラー システム

### POSIX準拠

- ▶ 広範囲に渡る POSIX API 仕様に対する POSIX PSE 52 サポート
- ▶ よく知られたプログラミング API と予測可能な動作
- ▶ ユーザーおよびグループ権限の正しい管理実践

### ハイ アベイラビリティと耐障害性

- ▶ 監視機能による障害の早期検出
- ▶ インテリジェントな再起動と自動再接続

### オープンな開発

- ▶ Foundry27 コミュニティを介し、QNX 開発者、ソース、フォーラム、プロジェクトロードマップにアクセス
- ▶ OS 技術のすべての主要エリアにおけるソースコードの可視性とアクセス。

### アダプティブ パーティショニング

- ▶ パフォーマンスや柔軟性に妥協せず、システム リソースの保障によりセキュアで信頼性の高いシステムを実現

### 予測可能なリアルタイムパフォーマンス

- ▶ 複数のスケジューリング メソッドに対応するプリエンティブなスケジューラ
- ▶ 優先度継承の分散機能

### マルチコア

- ▶ 総合的なマルチコア サポート
- ▶ 非対称型、対称型、限定型のマルチプロセッシング
- ▶ 単一処理から多重処理へのシームレスな移行

### 透過分散処理

- ▶ リモート リソースへの透過的なネットワーク アクセス
- ▶ 耐障害性に優れたシンプルなクラスタ設計

### ファイルシステム

- ▶ イメージ、RAM、フラッシュ、ディスク
- ▶ Linux、DOS、CD-ROM、DVD
- ▶ NFS、CIFS、圧縮
- ▶ パワーセーフなマス ストレージ ファイルシステム

### リソース マネージャ フレームワーク

- ▶ カーネル外のユーザー スペースでデバイス ドライバを実装
- ▶ 通常のアプリケーションと同様にドライバの起動停止およびデバッグが可能

### デバイス ドライバ

- ▶ オーディオ、キャラクタ、ディスク、グラフィックス、インプット、ネットワーク、パラレル、プリンタ、シリアル、USB

### プロセッサ サポート

- ▶ ARM、MIPS、PowerPC、SH-4、x86
- ▶ X86、MIPS、PowerPCにおける拡張メモリ サポート (4 GB 以上)

[www.qnx.co.jp](http://www.qnx.co.jp)