

Microchip 社、組み込みコントローラにハードウェア レベルの量子耐性を搭載

耐量子暗号、強化されたセキュリティ機能、低消費電力を特長とする MEC175xB ファミリ

2025 年 5 月 16 日[NASDAQ: MCHP] – 暗号研究の進展とより強固なセキュリティ対策の必要性を受け、米国 NSA(国家安全保障局)は、量子耐性を備えた暗号に関する一連の標準規格を定める事を目的とした CNSA 2.0 (Commercial National Security Algorithm Suite 2.0: 商用国家安全保障アルゴリズム スイート 2.0) を発表しました。NSA は現在、データセンターおよびコンピューティング市場に対し、今後 2 年以内に耐量子暗号への対応を完了するよう要請しています。進化するセキュリティ要件を満たすシステムの設計を支援するため、Microchip Technology Incorporated(日本法人: 東京都港区浜松町、代表: 樺晴彦 以下 Microchip 社)は本日、書き換え不可の耐量子暗号をサポートする [組み込みコントローラ MEC175xB](#) を発表しました。

スタンドアロン コントローラである MEC175xB ファミリは、モジュール式のアプローチを採用しており、効率的に耐量子暗号を導入して、既存の機能性を損なうことなく長期的なデータ保護を実現することができます。この低消費電力コントローラの設計には、米国 NIST(国立標準技術研究所)が承認した耐量子暗号アルゴリズム、設定変更可能なセキュアブート ソリューション、高度な eSPI(拡張シリアル ペリフェラル インターフェイス)が組み込まれています。

Microchip 社セキュリティ製品部門副社長の Nuri Dagdeviren は次のように述べています。「将来、量子コンピューティングによって暗号が破られる可能性があり、その重大さが広く認識され始めています。こうした状況を受け、サイバー セキュリティの潮流は既に大きく変わりつつあります。Microchip 社の MEC175xB コントローラは、書き換え不可のハードウェアに実装された耐量子暗号と効率的な電源管理を特長としており、複雑化するデジタルセキュリティ要件への対応に必要となる手段をお客様に提供します」

MEC175xB コントローラには、NIST によって標準化された CNSA 2.0 準拠の ML-DSA (Module-Lattice-Based Digital Signature Algorithms)、Merkle ステートフルハッシュベースの LMS (Leighton-Micali Signature)検証、ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)が組み込まれています。量子攻撃耐性を持つこれらの新しいアルゴリズムは、書き換え不可のハードウェアに実装されており、ソフトウェア実装の際に発生し得る攻撃経路を遮断します。

セキュアブートとセキュアファームウェア更新の方式を設定することで、CNSA 1.0、CNSA 2.0、またはハイブリッドベースの署名検証を利用できます。ML-DSA を用いたアステーション機能により署名と鍵生成を行い、システムの完全性と真正性を向上させます。コアには 96 MHz で動作する MPU(メモリ保護ユニット)搭載 Arm® Cortex®-M4F プロセッサを採用し、複雑な計算やリアルタイム アプリケーションに対応する高い性能を提供します。480 KB の SRAM、I3C®ホストおよびクライアント インターフェイス、USB 2.0 フルスピード インターフェイス (オプション)により、幅広い接続性を実現しています。

Microchip 社の [セキュリティ製品](#) ポートフォリオの詳細はウェブサイトをご覧ください。

Microchip 社、組み込みコントローラにハードウェアレベルの量子耐性を搭載

2-2-2-2

開発ツール

MEC175xB コントローラは、MPLAB® X IDE(統合開発環境)と互換性があり、SDE (Secure Document Extranet) で提供されている LED 点滅等のサンプルプロジェクトや、Zephyr®等の外部ツールでサポートされています。また、MEC1753-240 MECC (EV48H83A)開発ボードでもサポートされています。

価格と在庫/供給状況

MEC175xB コントローラは現在、Microchip 社のアーリーアダプタ プログラムで提供中です。詳細は Microchip 社の正規代理店にお問い合わせ頂くか、Microchip 社のオンラインストアのウェブサイト www.microchipdirect.com をご覧ください。

リソース

高画質の写真は報道関係専用窓口までお問い合わせ頂くか、Flickr でご覧ください。掲載に許可は不要です。

- アプリケーション画像: <https://www.flickr.com/photos/microchiptechnology/54456487663/sizes/o/>

Microchip Technology 社について:

Microchip Technology 社(以下、Microchip 社)はスマート、コネクテッド、セキュアな組み込み制御ソリューションおよび処理ソリューションのトッププロバイダです。使いやすい開発ツールと包括的な製品ポートフォリオにより、リスクを低減する最適な設計を作成し、総システムコストの削減、迅速な商品化を実現できます。Microchip 社は産業、車載、民生、航空宇宙と防衛、通信、コンピューティングの市場で 100,000 社を超えるお客様にソリューションを提供しています。Microchip 社は本社をアリゾナ州チャンドラーに構え、優れた技術サポート、確かな納期、高い品質を提供しています。詳細は Microchip 社ウェブサイト(www.microchip.com)をご覧ください。

###

Note: Microchip 社の名称とロゴ、Microchip ロゴは米国およびその他の国における Microchip Technology Incorporated の登録商標です。その他の商標は各社に帰属します。

詳細については、以下にお問い合わせください。

Daphne Yuen (Microchip 社):

(メール: daphne.yuen@microchip.com)

松田、仙場 (共同 PR):

(メール: mchp-pr@kyodo-pr.co.jp)

報道関係者の方へ: このニュースリリースのメールによる配信については、共同PR 株式会社松田もしくは仙場まで電話(03) 6260 4863 またはメール mchp-pr@kyodo-pr.co.jp でお問い合わせください。