

Microchip 社、CEC1736 リアルタイム プラットフォーム ルートオブトラストデバイスを加えて TrustFLEX ファミ리를拡充

幅広いアプリケーションでコンセプトから量産化までのルートオブトラストの実現を容易にする
TrustFLEX デバイスと Trust Platform Design Suite ツール

2024 年 3 月 27 日[NASDAQ: MCHP] - 技術とサイバー セキュリティ規格が進化し続ける中、Microchip Technology Incorporated(日本法人: 東京都港区浜松町、代表: 櫛晴彦 以下 Microchip 社)は本日、組み込みセキュリティソリューションをさらに利用しやすくする [CEC1736 TrustFLEX デバイス](#)を発表しました。CEC1736 Trust Shield ファミ리는データセンター、通信、ネットワーク、組み込みコンピューティング、工業用途のサイバーレジリエンスを実現するマイクロコントローラ ベースのプラットフォーム ルートオブトラスト ソリューションです。このたび、これらのデバイスは TrustFLEX プラットフォームの一部として Microchip 社の署名付き Soteria-G3 ファームウェアによって一部構成およびプロビジョニングされる事で、プラットフォーム ルートオブトラストの組み込みに必要な開発時間を短縮できるようになりました。これらのデバイスは必要な暗号化資産と署名済みのファームウェア イメージのプロビジョニングを迅速化し、NIST(米国国立標準技術研究所)と OCP (Open Compute Project)の規格で求められるセキュアな製造プロセスを簡略化するのにも役立ちます。

CEC1736 TrustFLEX デバイスは NIST 800-193 プラットフォームのレジリエンス ガイドラインと OCP の要件を満たすように特別に設計されており、各種市場でハードウェア ルートオブトラストを実現するために必要なセキュリティ機能をサポートしています。[Trust Platform Design Suite](#) ツールを使うと、独自の認証情報を含むプラットフォーム固有のコンフィグレーション設定をカスタマイズし、外部の SPI フラッシュ デバイスからブートする任意のアプリケーション、ホストプロセッサ、または SoC をサポートしてシステムのルートオブトラストを拡大できます。

「Microchip 社はあらゆる規模のデバイスとプラットフォームの設計から導入までのセキュアなプロビジョニングの効率化について業界をリードしてきました。このたび、その豊富なソリューションに OCP 準拠のルートオブトラストデバイスが加わりました」と Microchip 社セキュア コンピューティング部門副社長の Nuri Dagdeviren は述べています。「事前設定済みの CEC1736 TrustFLEX ファミリによって参入障壁が下がり、お客様はプラットフォーム ルートオブトラストを簡単に導入し、プロトタイピングを素早く実施して開発期間を短縮できるようになります」

SPI バス監視、セキュアブート、コンポーネント認証、ライフサイクル管理等、CEC1736 TrustFLEX で実現される最新のファームウェア セキュリティ機能により、ブート前環境とリアルタイム(TOC(チェック時点)およびTOU(利用時点))環境を現場での脅威と遠隔操作による脅威から常に保護できます。

Microchip 社、CEC1736 リアルタイム プラットフォーム ルートオブトラストデバイスを加えて TrustFLEX ファミリを拡充

2-2-2-2

柔軟に構成可能な先進のミクストシグナル I/O コントローラの CEC1736 は、32 ビット 96 MHz Arm® Cortex®-M4 プロセッサコアと密に結合されたメモリを搭載し理想的なコード実行とデータアクセスを実現します。

開発ツール

Microchip 社の包括的なツール エコシステムにより、設計を容易に開始できます。Trust Platform Design Suite の一部である CEC1736 TrustFLEX Configurator では各種ユースケースを視覚的に表示し、開発用、プロトタイプ用、量産用のプロビジョニング パッケージを選択、構成、生成できます。CEC1736 開発ボードには評価と開発を容易にするソケットが付属しています。

価格と在庫/供給状況

詳細とご購入は 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/53571550296/sizes//>
- ビデオは YouTube でご覧頂けます。掲載に許可は不要です。 <https://youtu.be/iaaCSdXqPcl>

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おおよそ 125,000 社の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、MPLAB 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。

Microchip 社、CEC1736 リアルタイム プラットフォーム ルートオブトラストデバイスを加えて
TrustFLEX ファミリを拡充

3-3-3-3

詳細については、以下にお問い合わせください。

Daphne Yuen (Microchip 社): (852) 2943 5115

(メール: daphne.yuen@microchip.com)

松田、仙場 (共同 PR): (03) 6260 4863

(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。