News Release

Microchip、システム プラットフォームでチェーンオブ トラストを実現する リアルタイム プラットフォーム ルートオブ トラストを発表

セキュリティに対する脅威からデータセンター、通信、ネットワークを保護する Trust Shield ファミリ

2022 年 5 月 18 日[NASDAQ: MCHP] – セキュリティに対する脅威が進化している今日、起動、リアルタイム動作、システム更新中の攻撃に対してプラットフォームの防御も進化する必要があります。新しい脅威によって設計に使う機器への信頼を前提とする事はできなくなり、システムを保護するための新しい技術を探す事が必要となりました。Microchip Technology Inc.(日本法人: 東京都港区浜松町、代表: 吉田洋介 以下 Microchip 社)は本日、設定変更可能なマイクロコントローラ ベースの CEC1736 Trust Shield ファミリを発表しました。本ファミリはシステム プラットフォームにチェーンオブ トラストを確立し、セキュアブート プロセスを実現するランタイム ファームウェア保護機能を使って NIST 800-193 プラットフォーム ファームウェア レジリエンス ガイドラインに準拠し、この課題を解決しています。

CEC1736 ファミリは最終製品のサイバー レジリエンス確保を支援します。CEC1736 は SPI フラッシュ内のファームウェアのランタイム保護と I^2C/SMBus のランタイム攻撃に対抗するフィルタ処理が可能な、設定変更可能なリアルタイム プラットフォーム ルートオブ トラストです。アテステーション機能は、プラットフォーム内のクリティカルなデバイスの真正性を保証する信頼可能な証拠を提供します。ライフサイクル管理と所有権移転機能を使う事で最終製品のライフサイクル全体にわたり、そして製品所有権移転時に秘密を保護でき、複数のオペレータが関わっても情報を漏えいさせずにシステム プラットフォームをセキュアに使用できます。

「もはや機器が信頼できる事を前提にはできません。周辺部品もファームウェア コンポーネントもその信頼性が証明されるまでは信用せず、不正であるかもしれないと想定し、それに対する防御を固める事が必要です」と Microchip 社コンピューティング製品部門担当副社長の Ian Harris は述べています。「Microchip 社の CEC1736 Trust Shield ファミリは、そのような課題に対する包括的ソリューションです。CEC1736 を使う事で製品化に要する時間を短縮でき、脅威に柔軟に対応できると同時に、開発と鍵のプロビジョニングをシンプルにできます。」

CEC1736 Trust Shield ファミリの先進のハードウェア暗号スイートは AES-256、SHA-512、RSA-4096、鍵サイズが最大 571 ビットまでの ECC、384 ビットの ECDSA(楕円曲線デジタル署名アルゴリズム)に対応しています。384 ビットのハードウェア PUF (Physically Unclonable Function)を使うと一意のルート鍵、対称秘密鍵、秘密鍵生成および保護が可能です。CEC1736 は NIST 800-193 および OCP セキュリティ ガイドラインに準拠しており、新しいセキュリティ技術および規格に迅速に対応できます。

CEC1736 Trust Shield ファミリはシリコン、ソフトウェア、ツール、開発ボード、エンドツーエンド プラットフォーム ファームウェア保護のためのプロビジョニング機能にまで及びます。

Microchip、システム プラットフォームでチェーンオブ トラストを実現するリアルタイム プラットフォーム ルートオブ トラストを発表
2 – 2 – 2

「セキュリティは事業継続性、消費者のプライバシー、国家安全保障にかかわる問題です。従って、セキュリティを保護する事は我々全ての責任です」と Kudelski IoT 社最高技術責任者であり IoT セキュリティの第一人者でもある Frédéric Thomas 氏は述べています。「Microchip 社は、同社のハードウェアを当社の先進セキュリティ ラボで当社と協力して客観的に評価する事で、CEC1736 Trust Shield ファミリが先進の攻撃方法に対して堅牢である事を確認しました。これにより、Microchip 社のお客様は、コネクテッド ワールドのセキュリティ全体に貢献するセキュアな最新マイクロコントローラを使って開発しているという安心感を得られるに違いありません。」

開発ツール

Microchip 社では CEC1736 Trust Shield ファミリ向けに使いやすい TPDS (Trust Platform Design Suite) を提供しています。機能を試し、セキュリティ設定の定義、試作および量産向けに秘密情報をプロビジョニングできる GUI コンフィグレータです。MPLAB® Harmony はデバイス設定、ライブラリ選択、アプリケーション開発を簡単にできる組み込みソフトウェア開発フレームワークです。他にも CEC1736 開発ボードを提供いたします。

在庫/供給状況

84 ピン WFBGA パッケージの CEC1736 96 MHz Arm® Cortex®-M4 ベース マイクロコントローラを含む CEC1736 Trust Shield ファミリは本日より受注を開始いたします。また、実績のある Soteria-G3 ファームウェア、CEC1736 開発ボード、そしてデバイスの設定、プロビジョニング、プログラミングを行う TPDS も提供いたします。
開発ボードは本日より受注を開始いたします。

- CEC1736 開発ボード(EV19K07A)

詳細は Microchip 社の正規代理店にお問い合わせ頂くか Microchip 社ウェブサイトをご覧ください。本プレスリリースに記載された製品をご購入頂くには、Microchip 社オンラインストアにアクセスするか、Microchip 社の正規代理店にお問い合わせください。

リソース

高画質の写真は 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/51990726338/sizes/l/

Microchip、システム プラットフォームでチェーンオブ トラストを実現するリアルタイム プラットフォーム ルートオブ トラストを発表
3 – 3 – 3

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 120,000 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。

###

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)

大川、仙場 (共同 PR): (03) 3571 5236
(メール: taito.okawa@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 大川もしくは仙場まで電話(03) 3571 5236 またはメール taito.okawa@kyodo-pr.co.jp でお問い合わせください。