

Microchip、ハードウェア ベースの IoT セキュリティを容易にする 少量生産にも対応したプロビジョニング済みソリューションを発表

Microchip 社が提供する Trust Platform はハードウェア ベースの
セキュアな鍵ストレージを少量生産から大量生産まで提供

2019 年 10 月 1 日[NASDAQ: MCHP]ーコネクテッド デバイスの数と種類が急増するにつれ、IoT 市場の細分化とセキュリティのぜい弱性が開発者に大きな課題となっています。ハードウェア ベースのセキュリティは物理的攻撃と遠隔不正アクセスから秘密鍵を保護する唯一の手段です。しかしデバイスを個別に設定、プロビジョニングするにはセキュリティに関する広範な専門知識、開発期間、コストが必要です。年間数百個から数百万個のコネクテッド デバイスを製造している企業が世界中に存在するため、アーキテクチャの拡張性が展開に対する大きな障壁になります。これまで、メーカーによる設定およびプロビジョニング サポートが受けられるのは大量発注できる企業に限られており、小～中規模の展開を行う企業には手順が煩雑な選択肢しかありませんでした。この需要に応えるため、Microchip Technology Inc. (日本支社: 東京都港区浜松町、代表: 吉田洋介 以下 Microchip 社)は本日、ATECC608A セキュア エLEMENTを使って小量から大量までのデバイス展開向けにセキュアな鍵ストレージを提供する業界初のプロビジョニング済みソリューションを発表しました。[Microchip 社の CryptoAuthentication™ファミリ向け Trust Platform](#)を使うと、展開する数量にかかわらず全ての企業がセキュア認証を簡単に実装できます。

Microchip 社の Trust Platform は数量規模に応じて 3 段階の製品で構成されています。そのまま使えるプロビジョニング済みセキュア エLEMENT、設定済みセキュア エLEMENT、フルカスタマイズ可能なセキュア エLEMENTです。この 3 つから、設計に最適なプラットフォームを選択できます。すぐに使えるセキュアな認証を大量市場に提供する初のソリューションとして、1 段階目である [Trust&GO](#) はゼロタッチ プロビジョニング済みセキュア エLEMENTです。最小注文数量(MOQ)は 10 個です。クラウドまたは LoRaWAN™認証オンボーディングを自動的に行うため、デバイスの認証情報は ATECC608A 内に事前書き込み、ロックされて出荷されます。同時に、証明書と公開鍵をマニフェスト ファイルで提供いたします。このファイルは Microchip 社のオンラインストアと一部の正規代理店経由で提供いたします。このソリューションは開発期間を数ヶ月も短縮節約できるだけでなく、プロビジョニング ロジスティクスを大幅にシンプルにできます。そのため、サードパーティのプロビジョニング サービスまたは認証関連の費用を使う事なく、量販市場向けのエッジデバイスを簡単に保護および管理できます。

いかなるパブリックまたはプライベート クラウド インフラストラクチャ向けでも認証可能な Microchip 社の Trust Platform は柔軟かつカスタマイズ可能でもあります。より大幅なカスタマイズを必要とするお客様のため、本プログラムでは TrustFLEX および TrustCUSTOM プラットフォームも提供しています。本プログラムの 2 段階目である [TrustFLEX](#)を使うと、設定済みユースケースの利点はそのままにして、お客様が選択した認証局を使えます。これらのユースケースは、認証チェーンを用いた任意の IP ベース ネットワークと接続するための TLS (Transport Layer Security)通信のハードウェア化された認証、LoRaWAN 認証、セキュアブート、OTA (Over-the-Air)更新、IP 保護、ユーザデータ保護、鍵ローテーション等の基本的なセキュリティ手段を含みます。

そのため、製品番号をカスタマイズする必要がなく、デバイスをカスタマイズするのに関わる時間と複雑さを低減できます。設計を全面的にカスタマイズする必要がある場合、本プログラムの 3 段階目である [TrustCUSTOM](#) がカスタム設定機能および認証情報プロビジョニング機能を提供します。

「ソフトウェア ベースのセキュリティソリューションに対する攻撃の成功件数の増加は、セキュア エLEMENT 内での秘密鍵の隔離を含む業界のベスト プラクティスを採用する必要性を明確に示しています」と Microchip 社セキュア製品部門副社長の Nuri Dagdeviren は述べています。「Microchip 社の Trust Platform は、実装する数量にかかわらず、あらゆる企業に簡単かつ低コストでハードウェア ベース セキュリティを提供し、デバイスの設定とプロビジョニングに関わる従来の障壁を取り除きます。」

Microchip 社は Microchip Trust Platform で設計した製品向けに、AWS (Amazon Web Services) と協力して AWS IoT サービスへの簡単なオンボーディング プロセスを実現しました。

ATECC608A はコモン クライテリアの JIL (Joint Interpretation Library 作業部会) で「高」評価を得ているセキュアな鍵ストレージ機能を備えており、実証済みのセキュリティ手法と最高水準のセキュアな鍵ストレージを実装していると信頼できます。本デバイスはハードウェア ベースのルートオブトラスト(信頼の基点) ストレージおよび暗号対策を実装しており、既知の物理攻撃に対して最も幅広く保護されています。Microchip 社のセキュアな製造施設は鍵を安全にプロビジョニングしており、プロビジョニング中またはフィールドで鍵が暴露される事のないようにしています。

開発ツール

ATECC608A は、いかなるマイクロコントローラおよびマイクロプロセッサとも組み合わせる事ができます。セキュア ソリューションを素早く試作できるように、以下を含む Trust Platform 設計スイートを提供しています。

- ガイド付き「ユースケース ツール」
- Jupyter Notebook で動作する Python チュートリアル
- 各ユースケースの C サンプルコード
- 「秘密鍵交換」ユーティリティ
- Trust Platform ハードウェア開発キット

在庫/供給状況

Microchip 社の Trust Platform のデバイスは、以下の最小注文数量(MOQ)で、本日より量産出荷を開始いたします。

- TLS 向け [Trust&GO](#) (ATECC608A-TNGTLSx-B): MOQ = 10 個*
- TLS 向け [Trust&GO](#) (ATECC608A-TNGTLSx-G): MOQ = 2,000 個*
- LoRaWAN 向け [Trust&GO](#) (The Things Industries 社 ATECC608A-TNGLORAx-B、Actility 社 ATECC608A-TNGACTU-B): MOQ = 10 個*
- LoRaWAN ジョインサーバ向け [TrustFLEX](#) (ATECC608A-TFLXLORAx): MOQ = 2,000 個*
- [TrustFLEX](#) (ATECC608A-TFLXTLSx): MOQ = 2,000 個*

- [TrustCUSTOM](#) (ATECC608A-TCSTMTLSx): MOQ = 4,000 個*
*uDFN (x = U)または SO8 (x = S)

Microchip 社の Trust Platform では以下の開発ツールを提供しています。

- CryptoAuth Trust Platform キット
- ATECC608a Trust Platform キット

詳細と製品のご購入は Microchip 社の [purchasing portal](#) にアクセスするか、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/48650099116>
- ツールの写真: <https://www.flickr.com/photos/microchiptechnology/48631110133>

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半導体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 125,000 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(<http://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): (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。