

## Microchip、IP の保護とセキュアなコネクテッド システムの展開を支援する CryptoAuthentication™デバイスとセキュリティ デザイン パートナー プログラムを発表

ATECC608A とセキュリティ デザイン パートナー プログラムにより、  
セキュアなソリューションの設計に必要なデバイスとパートナーを提供

2017 年 11 月 21 日[NASDAQ: MCHP] – リモートからのサイバー攻撃や偽造品の製造等、セキュリティの脅威は多岐にわたり、あらゆる産業に影響を与えています。これらの脅威が現実のものになれば、復旧コストやサービス収益、そして恐らく最も重要な点としてブランド資産価値に甚大な損失が生じる可能性があります。知的財産(IP)を保護し、ネットワークに接続した機器の信頼できる認証を確保するには、設計に強力なセキュリティを組み込む事が不可欠です。こうした脅威を防ぐため、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、CryptoAuthentication™ファミリ ATECC608A を発表しました。これにより、ハードウェア ベースのセキュリティを回路設計に追加できます。また、開発者とサードパーティ パートナーをつなぎ、短期間でよりセキュアな設計を可能にするセキュリティ デザイン パートナー プログラムも開始しました。Microchip 社の最新セキュリティソリューションの詳細は <http://www.microchip.com/design-centers/security-ics/cryptoauthentication/overview> を参照してください。

通信セキュリティの基盤は、デバイス固有の信頼済みアイデンティティを作成、保護、認証する機能で構成されます。デバイスの秘密鍵をシステムから隔離されたセキュアな領域に格納でき、業界最先端の暗号手法を採用した ATECC608A は、ほぼ全種の設計に使える高度なセキュリティを提供します。ATECC608A の主な機能は次の通りです。

- **クラス最高の鍵生成:** FIPS(連邦情報処理標準)準拠の乱数生成器(RNG)を使って、NIST(米国国立標準技術研究所)の最新要件を満たした一意の鍵を生成します。このため、システムレベルでの FIPS 認証も容易に取得できます。
- **小規模システム向けのブート検証機能:** ARM® Cortex®-M0+等の小型 MCU を使ったシステム、およびより高いロバスト性が要求される組み込みシステムでは、新しいコマンドを使ってホスト マイクロコントローラ(MCU)のファームウェアに対する署名検証とダイジェスト計算が容易に行えます。
- **LoRa ノードに対する認証の信頼性:** AES-128 エンジンによりネットワーク内の信頼済みノードを認証できるため、LoRa インフラストラクチャにもセキュリティを導入できます。
- **高速暗号処理:** ハードウェア ベースの楕円曲線暗号(ECC)アルゴリズムを内蔵しているため生成する鍵長が短く、レガシー手法に基づく実装アプローチよりも迅速かつセキュアに証明書ベースの Root of Trust(信頼の起点)を確立できます。
- **耐タンパー保護機能:** 各種の耐タンパー手法により、運用開始後の物理的攻撃および侵入攻撃から鍵を保護します。これらの手法により、システムはセキュリティ保護された信頼済みアイデンティティを維持できます。

- **信頼済み製造施設でのプロビジョニング:** Microchip 社のセキュアな製造施設でメーカーが鍵と証明書を安全にプロビジョニングできるため、製造段階での漏洩リスクをなくせます。

「今日のコネクテッド アプリケーション、それも特にハードウェアからクラウドまでをカバーするのはセキュリティが不可欠です」と Microchip 社セキュア製品部門副社長の Nuri Dagdeviren は述べています。「実証済みのハードウェア セキュリティ ソリューションに加え、主要なクラウド プロバイダとの過去最大規模のパートナー プログラムを Microchip 社が発表したのはこのためです。これにより、お客様は IP、ブランド価値、収入源を保護するセキュアなソリューションの開発に必要な全ての要素を手にして頂く事ができます。」

ハードウェア セキュリティ ソリューションの提供に加え、Microchip 社はこのたび**セキュリティ デザイン パートナー プログラム**も開始しました。Amazon Web Services (AWS)や Google Cloud Platform 等、業界をリードするパートナー企業が補完的なクラウド駆動型のセキュリティ モデルとインフラストラクチャを提供します。パートナー各社は Microchip 社のセキュリティ デバイスおよびライブラリの実装に精通しています。IoT (Internet of Things)アプリケーションのセキュリティを確保したい場合や、カートリッジ等の消耗品またはアクセサリ品に認証機能を追加したい場合にセキュリティ デザイン パートナーの高度な知識と経験を活かすと、開発コストおよび期間を圧縮できます。

「Microchip 社との協業を通じて ATECC608A の作業に携わったため、Google IoT のお客様は高度なセキュリティを備えたこの新製品をすぐに使いこなして頂く事ができます」と Google Cloud IoT プロダクト マネジメント リードの Antony Passemard 氏は述べています。

## 開発ツール

セキュア ソリューションのラピッド プロトタイピング向けに CryptoAuth Xplained Pro 評価および開発キット (ATCryptoAuth-XPRO-B)を提供いたします。このアドオンボードは Microchip 社の Xplained および XplainedPro 評価用ボード全製品と互換です。

## 在庫/供給状況

ATECC608A は本日より量産出荷を開始いたします。ATCryptoAuth-XPRO-B アドオン開発ボードも本日より提供いたします。

詳細は Microchip 社または正規販売代理店にお問い合わせください。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 社のオンラインストア [microchipDIRECT](https://www.microchip.com/direct) にアクセスするか、Microchip 社の正規販売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)。

- PR 画像: [www.flickr.com/photos/microchiptechnology/38318249271](https://www.flickr.com/photos/microchiptechnology/38318249271)
- 製品画像: [www.flickr.com/photos/microchiptechnology/38318249941](https://www.flickr.com/photos/microchiptechnology/38318249941)
- ブロック図: [www.flickr.com/photos/microchiptechnology/38318249431](https://www.flickr.com/photos/microchiptechnology/38318249431)

## Microchip 社について

Microchip 社(NASDAQ:MCHP)は、マイクロコントローラ、ミックスドシグナル、アナログ、Flash-IP ソリューションのトッププロバイダであり、全世界で数千を超える各種アプリケーションで、低リスクの製品開発、総システムコストの削減、迅速な商品化の実現に貢献しています。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 社のウェブサイト (<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。ARM、Cortex は EU およびその他の国における ARM Limited の登録商標です。その他本書に記載されている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](mailto:daphne.yuen@microchip.com))

大川、仙場 (共同 PR): (03) 3571 5236  
(メール: [taito.okawa@kyodo-pr.co.jp](mailto: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](mailto:taito.okawa@kyodo-pr.co.jp) でお問い合わせください。