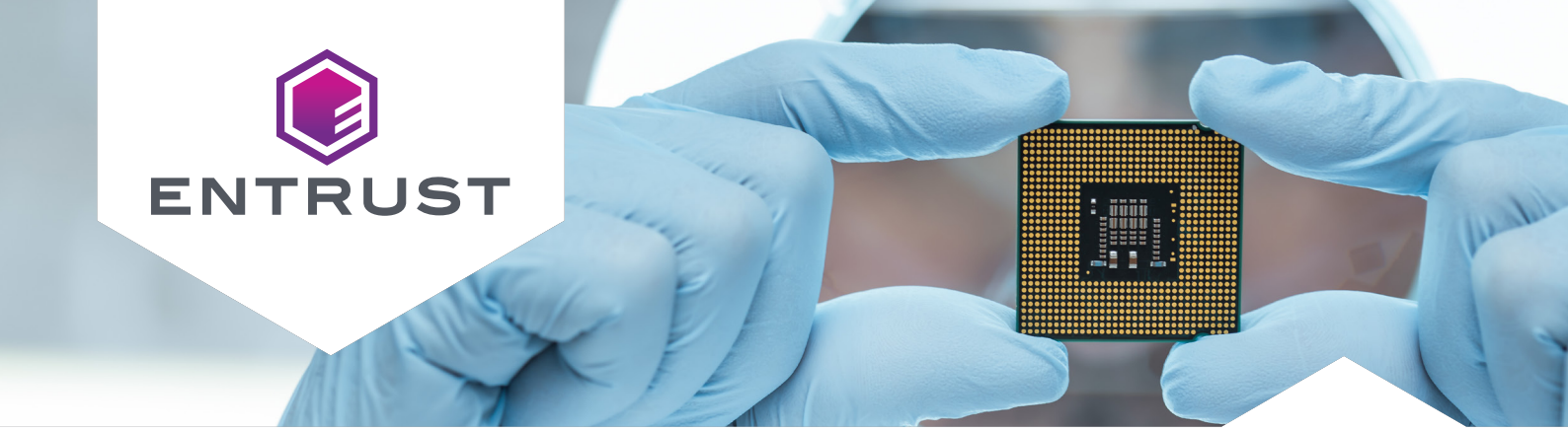

EntrustがMicrochipのIoT対応SAM L11マイクロコントローラのルートIDをプロビジョニング

モノのインターネット（IoT）は、もはや止めることのできない現象になっています。IDCは、接続されたIoTデバイスの総数が2025年までに400億を超えると予測しており、多くの人が、この予測は非常に控えめな数であると見なしています。

しかし、自動運転車からスマート家電、ヘルスケア機器、農業機械に至るまで、IoT関連のエンドポイントの爆発的な急増に伴い、ユニークな課題が生まれています。これらの中で最も重要な課題となるのは、セキュリティに関する問題で、すべてのデバイスが不正アクセスから保護されていることを保証する必要があります。

ビジネスニーズ

Microchip Technologyの製品マーケティング担当部長であるAnand Rangarajan氏は、次のように述べています。「現在、IoTの領域には、セキュリティに関する一般的な基準が存在していない。適切なセキュリティ対策を製品に組み込むことは非常に複雑で、多くのメーカーにとって悩みの種となっている」

> **強力な産業用セキュリティを組み込みシステムに統合することで、IoT市場全体に大きな変革をもたらした**
>
> – Microchip Technology製品マーケティング担当部長、Anand Rangarajan氏

詳細をチェック：ENTRUST.COM/ja/HSM

Microchip

Microchip Technology, Inc.は、前例のない革新的な製品を生み出し続けることで知られており、マイクロコントローラ、ミックスドシグナル、アナログ、フラッシュIPソリューションの世界有数のプロバイダーです。同社の最新マイクロコントローラの1つであるSAM L11は、ARM Techconにおいて、「2018 Innovation Award for Best Contribution to IoT Security」を受賞しました。具体的な性能として、IoTノードと、医療機器、センサー、カメラ、自動車といった、スマートエンドポイントの機能やセキュリティに関するニーズに対応します。

アリゾナ州チャンドラーに本社を置くマMicrochipは、ナスダック取引所で上場しています。同社は、数十億個のマイクロコントローラとマイクロプロセッサを、世界中の数十万人の顧客にお届けしてきました。

技術的ニーズ

「マイクロコントローラの観点からSAM L11のユースケースを予想すると、高性能でありながら低消費電力を達成することなど、非常にユニークな設計上のニーズが浮き彫りになる」と、Rangarajan氏は説明します。

ソリューション

SAM L11のセキュリティアーキテクチャの中心となるのは、製造中にデバイス固有の鍵を挿入できるようにするためにMicrochipによって開発された、信頼の基点機能です。重要なタスクを管理・実行するためのテクノロジーの選択は、非常に簡単であることが証明されました。「当社はEntrust（旧称：nCipher）と長年にわたって提携しており、個々の鍵を生成するために同社のハードウェア・セキュリティ・モジュール（HSM）を選択したことは、当社にとって当然のことだった」と、Rangarajan氏は述べています。

Entrust nShield® HSMは、重要な暗号化、デジタル署名、鍵生成機能を実行する認定ハードウェアセキュリティアプライアンスです。この強化されたネットワークプラットフォームは拡張性に優れており、独自の柔軟なアーキテクチャを利用して、業界をリードする暗号化トランザクション率を実現します。

効果

「nShield HSMから各SAM L11マイクロコントローラに一意の鍵を挿入することができるため、デバイスを個別に識別・検証し、リモートで管理することができる。これは、IoTデバイスと他の接続されたエンドポイントの間で信頼を再確立する必要がある場合に特に重要である」と、Rangarajan氏は述べています。「製造業者は、クラウドを最大限に活用して、各ノード間に安全かつ広範な接続を提供できるようになった。同HSMは、ワイヤレスセンサーの保護、ハンドヘルド型医療機器のデータの暗号化、さらには、クラウド接続型システムのリモート認証といったアプリケーションに最適です。」

Microchip SAM L11マイクロコントローラの非常に説得力のある価値設定が実現した一つの要因には、世界中で15億個以上ものシステムを保護しているデバイスセキュリティ市場のリーダー企業、Trustonicとの提携が挙げられます。

Trustonicは業界最大の技術的進歩の1つとも言える、認証、セキュアブート、改ざん検出、AESおよびSHA暗号化、セキュアキーストレージといったセキュリティ機能のライブラリを開発し、これは、ソフトウェア開発キットに組み込まれています。

Microchip

> **個々の鍵を生成するためにEntrust nShield HSMを選択したことは、当社にとって当然のことだった**
>
> – Microchip Technology製品マーケティング担当部長、Anand Rangarajan氏

「設計者は、モジュラーセキュリティフレームワークを使用して簡単なAPI呼び出しを行い、構築した非常に高度なセキュリティ機能のセットにアクセスできるようになった」と、Rangarajan氏はコメントしています。「チップレベルのプロトコルに関する深い専門知識はもはや必要ない。これにより、開発期間が大幅に短縮され、従来、IoTデバイスのセキュリティ保護に関連して発生していた経費を大幅に削減できる」

セキュリティモジュールのライブラリは、サイズに制約のあるIoTチップセット用にTrustonicによってカスタム設計され、ハードウェアで保護されたモジュラー型オペレーティング環境、Kinibi-Mの上に構築されています。Kinibi-Mの下にあるハードウェア抽象化レイヤーは、Entrust nShieldで生成された暗号鍵の使用の管理など、SAM L11との直接通信を円滑にします。

「MicrochipのSAM L11開発者は、独自のデューデリジェンスを行って、Entrust nShield HSMが当社にとって最適な選択肢であると判断したが、それとはまったく関係なく、TrustonicもEntrust HSMを使用するよう当社に推奨してきた。このように、まったく別のところから当社の決定に対して支持を得たことで、当社の意思はさらに硬いものとなった」と、ランガラジャンは回想しました。

革新的なチップによりセキュリティを簡素化

SAM L11は、Arm Cortex-M23とArm TrustZone搭載のセキュリティテクノロジーを利用した、業界初のマイクロコントローラです。信頼できるリソースと信頼できないリソースをハードウェアによって強制的に分離します。Rangarajan氏は、次のように述べています。「セキュリティアーキテクチャは洗練された包括的な機能を備えつつも、Kinibi-Mを使用することにより、SAM L11のセキュリティ機能と完全に統合されたファームウェアによって、容易かつ安全なアプリケーション開発を実現する。また同時に、SAM L11などのデバイスからメリットを得うる、関連したIoTユースケースに対処するためのコード例を提供する」

Entrust nShield® HSMによって生成された鍵を利用して、世界レベルの信頼の基点となる基盤をIoTデバイス開発者に提供する機能は、世界的に大きな影響を与えています。Rangarajan氏は、次のように述べています。「当社が採用したアプローチは、消費電力が非常に少ない高性能パッケージに、セキュリティを組み込むことができるようになったことを意味している。強力な産業用セキュリティを組み込みシステムに統合することで、IoT市場全体に大きな変革をもたらした」

Microchip

IoT全体のセキュリティを変革

ビジネスニーズ

- IoTノードとエンドポイントを保護するためのソリューションを作成
- IoTデバイスにセキュリティを組み込む際の複雑さとコストを削減
- 専門的なチップレベルのプログラミングスキルの必要性を排除

技術的ニーズ

- 高速かつ電力効率に優れたマイクロコントローラに堅牢なセキュリティ機能を統合
- 小さなフットプリントを設計し、メモリを大量に消費するアプリケーションでの使用を可能に
- 信頼の基点を確立

ソリューション

- Entrust nShield HSM

効果

- 業界をリードする機能と性能を備えたSAM L11マイクロコントローラの発表
- ソフトウェア開発キットにより、高度なセキュリティ機能へのシンプルなAPIアクセスを提供
- IoTデバイス製造業者による製品の市場投入までの時間の短縮
- IoTデバイスおよびそれらが生成するデータの信頼性を確立

ENTRUSTについて

Entrust は信頼される認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com