STSAFE-Aを使用して ネットワーク·サービスに接続する 機器を保護する方法

目次

コネクテッド·デバイス市場の概要

監視カメラ、給水ポンプ、熱モニタ。これらの共通点は、ネットワークに接続されるようになったことです。自宅でも、都市部でも、産業インフラでも、コネクテッド·デバイスはあらゆるところに存在します。この「これまでにないコネクティビティ」の波に拍車をかける要因は複数ありますが、その中で特に重要なのが、販売手法の変化です。

従来型のビジネス·モデルから…

以前は、機器は店舗で販売されていました。いくつか利点がある一方で、欠点も多数ありました。特に重大な欠点は、機器販売による収益の発生は1回限りであること、そして企業にとって顧客の使用体験からのフィードバックが得られにくいことでした。

…サービスベースのアプローチへ

こういった状況を観察してきた結果、企業はビジネス·モデルを拡大し、経常的に発生する付加的なサービスを販売するようになりました。このアプローチには企業にとって経常収益を確保できる利点があります。また、顧客をさらに囲い込み、最終的に顧客からの直接的なフィードバックを得る手段にもなりました。

新しい技術の急成長により実現

このビジネス·モデルの進化が実現に至ったのは、さまざまな新技術が登場したからです。その中でも特に重要なのが、ネットワーク接続型機器とセンサ / アクチュエータ、クラウドでのデータ処理、人工知能（AI）です。

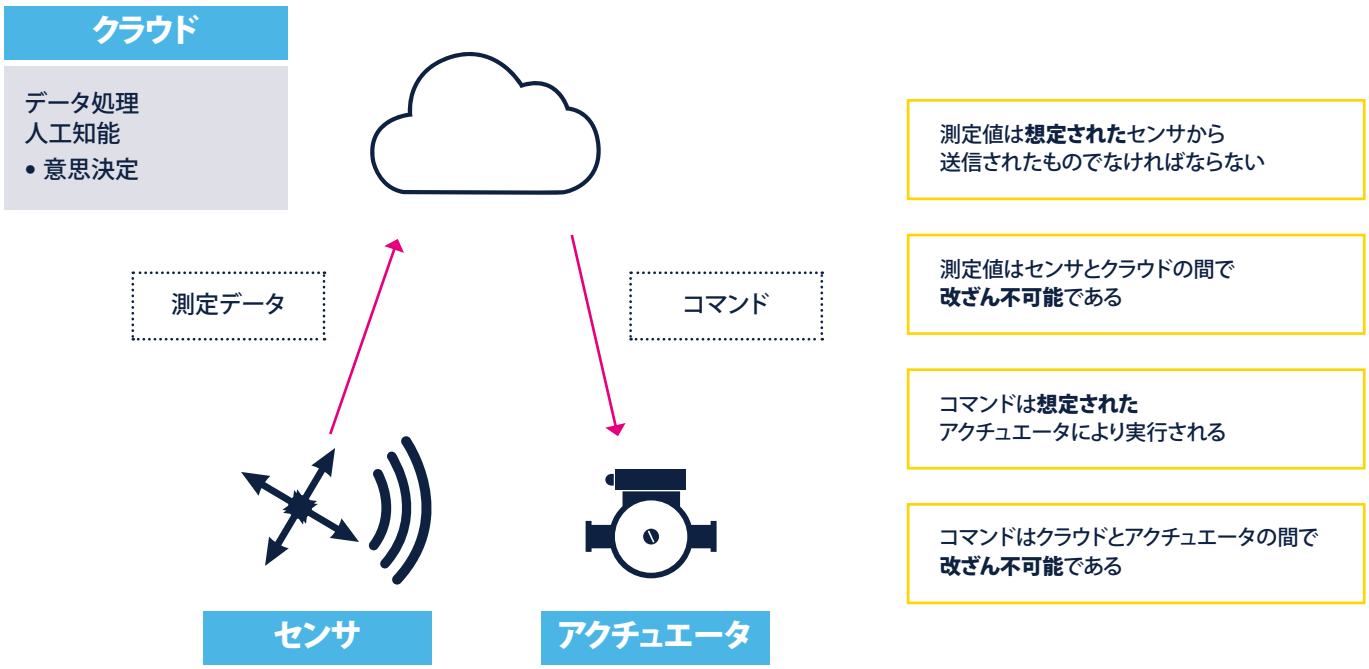
コネクテッド·デバイスの原則について

サービス·ベースのビジネス·モデルが成立する条件

このビジネス·モデルが成立するには、次の3つの条件を満たす必要があります。

- サービスが利用できる状態であること
- サービスが信頼できる状態であること
- サービスは顧客情報のプライバシーを保証すること

この構成では、顧客はサービスに対して代金を支払います。そのため、品質に対する期待値が高い点にも注意が必要です。



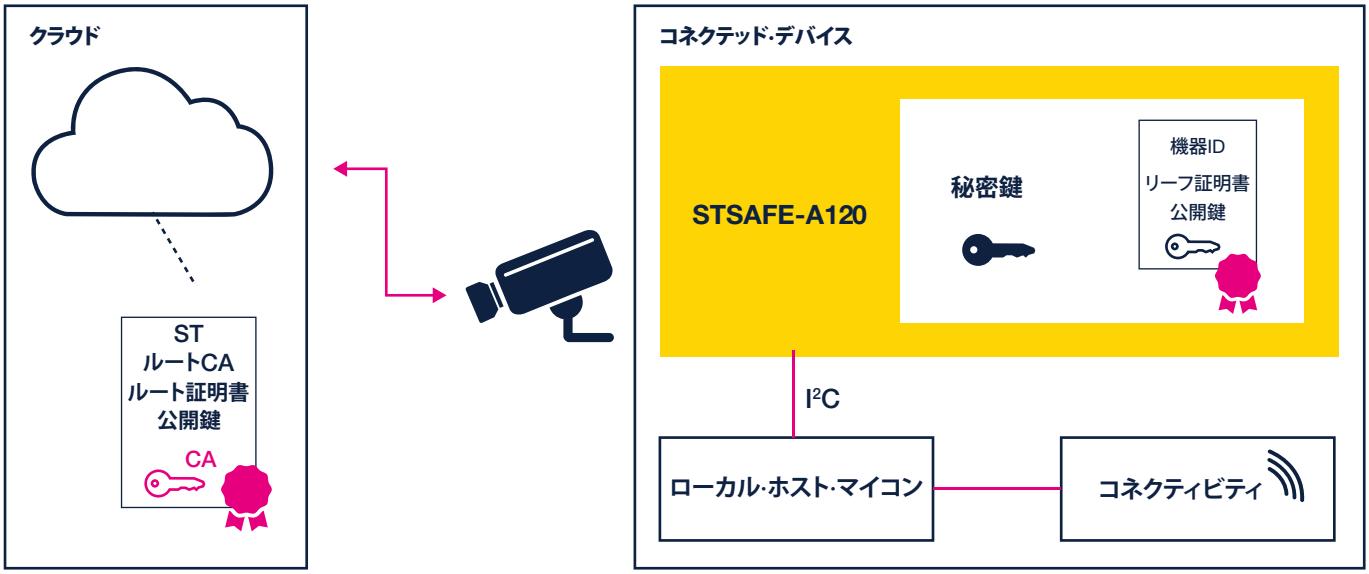
この4つの要件を確実に満たすために、次の2つのプロセスを実装できます。

- **センサとアクチュエータの認証:** 測定値が想定されたセンサから送信されたものであること、コマンドが想定されたアクチュエータにより実行されることの両方を保証するために、このソリューションでは両方の機器を認証します。
- **データとコマンドの署名、暗号化:** 測定値がセンサとクラウドの間で改ざん不可能であること、コマンドがクラウドとアクチュエータの間で改ざん不可能であることの両方を保証するために、このソリューションではデータとコマンドに署名し、それらを暗号化します。

認証ソリューション「STSAFE-A」の導入

STSAFE-Aの概要

STSAFE-Aは、対象機器のセキュアな認証を可能にするソリューションです。独立した第三者機関による認定を取得したセキュア・エレメントをベースとし、機器の認証を実行し使用状況をモニタリングするために設計されたコマンド・セットを備えています。



製品認証用に最適化されたシステム・オン・チップ（SoC）

STSAFEには秘密鍵とX509証明書が組み込まれているため、対象機器の厳格な認証が可能です。また、認証用にセキュリティ・プロトコルを実装するための基本APIも含まれています。

対象機器のローカル・ホスト・マイコン / MPUのコンパニオン・チップ

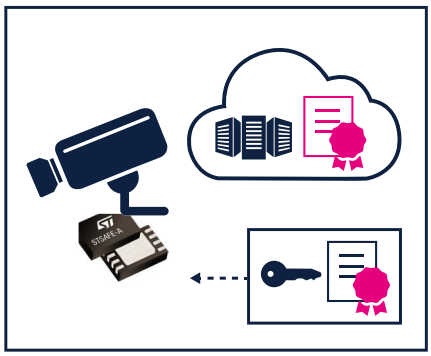
STSAFE-AはシンプルなI²Cインタフェースを介してローカル・ホストに接続します。

STのセキュアな製造拠点でパーソナライズ

STSAFE-Aは、顧客固有の対象機器の秘密情報やその他の情報について、STのセキュアな製造拠点でパーソナライズ書込みできます。

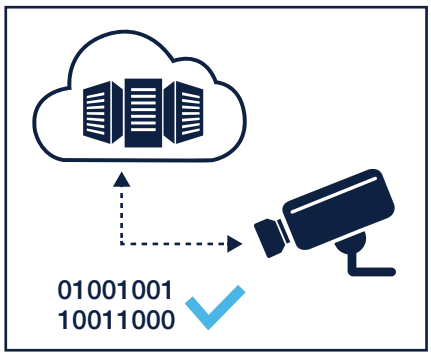
製品機能

クラウドとのセキュアな接続を確保するため、STSAFE-Aは次の4つの主要タスクを実行するように設計されています。



機器の認証

STSAFE-Aは、機器を認証するためのX509証明書とセキュリティ・プロトコルが組み込まれた状態でお客様に届けられます。

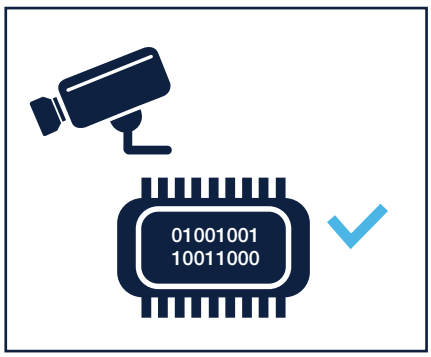


クラウドとのセキュアな接続の確立

STSAFE-Aは、交換データの署名や暗号化によってデータの完全性と機密性を保証します。たとえば、監視カメラとクラウドベース・サーバの間で交換されるデータに署名し、同時にそのデータを暗号化できます。

接続用の認証情報と機密データのセキュアな保存

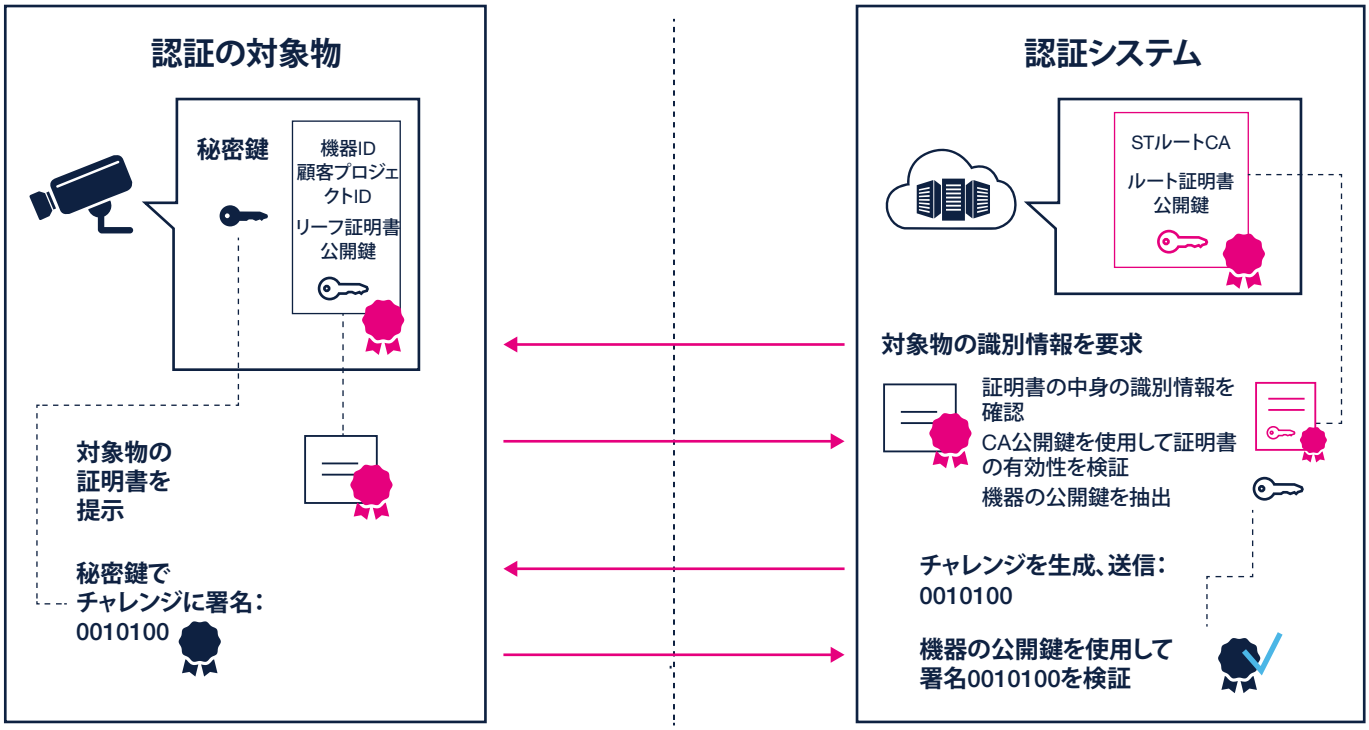
STSAFE-Aを利用して、認証情報や機密データをセキュア・エレメント（SE）のストレージや機器の不揮発性メモリ（NVM）にセキュアに保存できます。



機器のファームウェアとアップデートの完全性検証

STSAFE-Aは、最初の起動時とファームウェアの更新時に、機器のアプリケーション・ファームウェアの署名を検証します。

認証プロセスの仕組み



STSAFE-Aは、認証が必要な対象物（この例ではカメラ）に組み込まれるセキュア・エレメントです。このセキュア・エレメントにカメラの証明書が格納され、この証明書に公開鍵と秘密鍵が含まれています。これに対して、クラウドは認証システムとして動作し、認証局（CA）と公開鍵を保持します。

クラウドによるカメラの認証方法

1.はじめに、クラウドはカメラに対して対象物の識別情報を要求します。
2.カメラはクラウドに証明書を提示します。
3.クラウドは独自のCA公開鍵 を使用して、その証明書の有効性を検証します。
4.有効性が証明された場合、クラウドはカメラの証明書から公開鍵 を抽出します。
5.クラウドはチャレンジを生成し、カメラに送信します。
6.カメラは秘密鍵 を使用してこのチャレンジに署名し、クラウドに返信します。
7.最後に、クラウドはカメラの証明書から抽出しておいた公開鍵 を使用して、
このチャレンジの署名を検証します。

**認証完了済みの
クラウドが想定するカメラ**

セキュリティ堅牢性の確保
STAFE-A

認定取得済みの最先端のセキュリティにより秘密情報を保護

STSAFE-Aは、銀行カードやデジタルIDで使用されている技術と同様の最新のセキュリティ技術をベースとしています。STSAFE-Aは、物理的な攻撃、論理的な攻撃の両方と効果的に戦うための高度な対抗措置を組み込んだセキュア・エレメントです。

セキュリティ対策	リモートからの攻撃に対する保護	チップへの攻撃に対する保護	広く認知されている外部機関による認定

STのセキュア・エレメント、その開発環境および製造プロセスは、独立した外部の検証機関や認証機関による定期的な監査と認定を受けています。

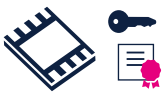
これらの独立機関により、STのソリューションが最も厳格なセキュリティ標準に準拠していることが確認されています。たとえば、STSAFE-A120はCommon Criteria（CC）EAL5+ AVA_VAN5の認定を取得済みです。

ST拠点でのセキュアなプロビジョニング

STSAFE-Aは、機器の秘密情報や証明書について、STのセキュアな製造拠点でパーソナライズできます。このサービスは、最小オーダー数（MOQ）5,000個から対応可能です。

チップの開発と
パッケージング

顧客情報による
パーソナライズ



ユーザへの出荷

機器メーカーや消耗品メーカーにとっての利点

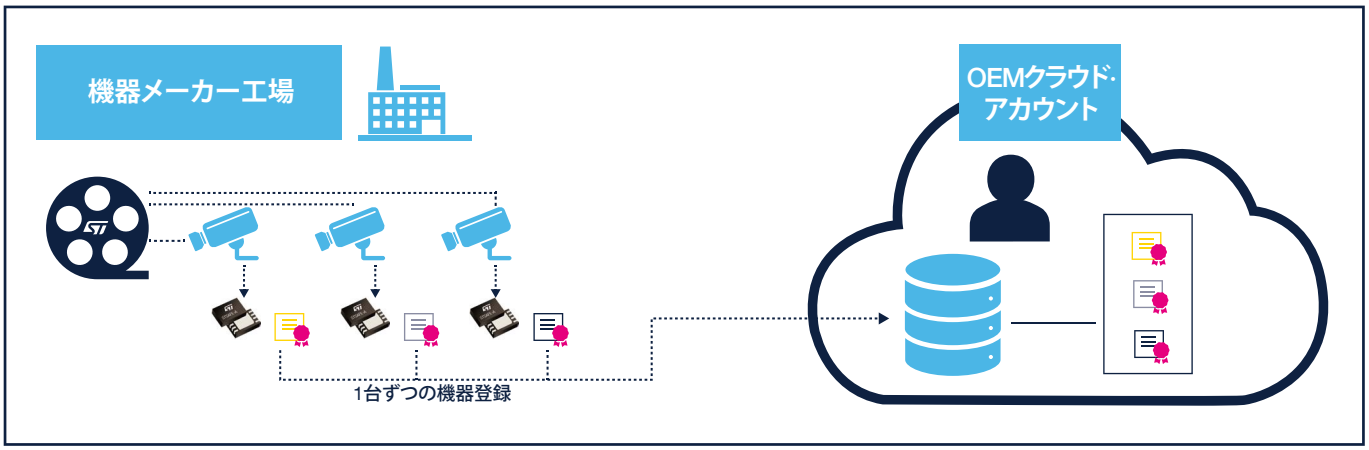
- 機密データや秘密情報の改ざん不可
- メーカーの製造ラインに対する個別の投資が不要
- セキュリティ・スキル習得のための個別の投資が不要
- オンライン・データ・ローディングが不要
- 製造停止のリスクなし
- メーカーはセキュリティに不安を感じることなく外部のパートナーやEMSを選択可能

STSAFE-Aによる ネットワーク接続型機器の クラウド·アカウント登録

ネットワーク接続型機器をベースとしたサービスのセキュリティは、そのサービスによって機器を厳格に認証できるかどうかにかかっています。この認証では、OEMが機器を市場向けに販売する前に、機器を対象のサービスに登録する必要があります。機器は1つずつ登録することも、ファミリ全体をあらかじめ登録することもできます。

機器1台のクラウド·アカウントへの登録

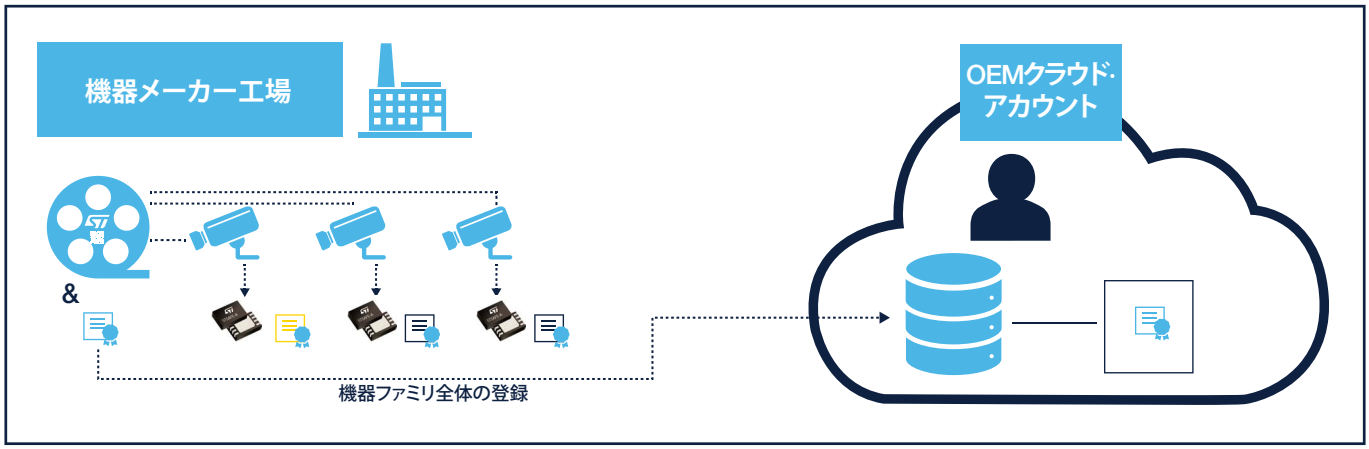
STSAFE-Aのそれぞれに X509証明書が搭載されており、この証明書には認証用の一意のIDと鍵が含まれています。このX509証明書を持つクラウド·アカウントは、この証明書を使用して、STSAFE-Aを搭載したコネクテッド·デバイスを厳格に認証できます。各機器のX509証明書をこのクラウド·アカウントに登録することで、その機器を登録できます。



機器ファミリ全体のクラウド·アカウントへの登録

機器ファミリ証明書を1つ登録することで、機器ファミリ全体をクラウド·アカウントに登録できます。

機器メーカーは、最小オーダー数(MOQ)5,000個から、このファミリ証明書の発行をSTに依頼できます。これにより、機器メーカーはSTSAFE-A X509証明書を1台ずつ読み取る必要がなくなります。



まとめ

STSAFE-Aは、認定取得済みの最先端のハードウェア・セキュリティをベースとして最適化されたシステム・オン・チップ（SoC）であり、機器認証のためのシンプルなソリューションを提供するセキュア・エレメントです。

高いセキュリティ・レベルを維持するために、STSAFE-Aは機器の情報（X509証明書）について、STのセキュアな製造拠点でパーソナライズできます。

さらに、STから提供するハードウェア / ソフトウェア・エコシステム一式により、セキュリティに関する特別な知識のない機器メーカーでも容易に実装できます。

詳細情報について

ST製品の詳細はこちら

STのセールス・オフィスへのお問い合わせや販売代理店検索はこちら

At STMicroelectronics we create technology that starts with You

MIX
Paper from responsible sources
FSC® C003379

Order code: **BR2404STSAFEACDEVJ**

詳細は ST ウェブサイトをご覧ください：www.st.com

ST マイクロエレクトロニクス株式会社
■東京 TEL 03-5783-8200 ■大阪 TEL 06-6397-4130 ■名古屋 TEL 052-587-4547