life.augmented

STSAFE™
IoT向けセキュア・ソリューション

目次

IoTとは

ビジネスを保護：セキュアで信頼できる組込みシステムの構築

世界経済の動向により、様々な企業がそのビジネスモデルを変化させています。IoTの登場により、接続されたオブジェクトのデータ使用や関連サービスの収益化を通して、企業には新しいチャンスが開かれています。企業イメージは製品とサービスの質で決まります。企業の評価は、セキュアで信頼の置けるソリューションを提供する能力にかかっています。

この新しい環境では企業の資産が新しい脅威に晒されるケースが大幅に増加する可能性があるため、もはやセキュリティはオブジェクト・レベル（個々のデバイス）で考えるだけではなく、システム・レベルやプラットフォーム・レベルまでを含む必要があります。単純なセキュリティの誤りや不正確なデータの測定によりサービス拒否が発生すると、エンド・ユーザの安全やプライバシーに影響をもたらし、企業ブランドの評判を損なう可能性があります。

企業が評判を維持しブランドを保護するためのサポートとして、STは製品とソリューションの幅広いポートフォリオや、ハードウェアおよびソフトウェア開発ツールを提供しており、企業の組込みシステムによって測定されるデータの正確性の提供と、セキュアな方法で正しく処理されることを保証しています。

IoT市場 & アプリケーション

セキュア組込みシステムの市場は現在拡大を続けており、広く利用されているブランド保護、ITセキュリティ、およびTPMソリューションから、IoT用のコネクテッド・デバイスまで幅広く含むようになっています。Smart meter、Smart City、Smart Home、およびIndustry 4.0イニシアティブを含むSmart Industryに関係するコネクテッド・デバイスから送信されるデータは、高い信頼性が必須です。プリンタ、PC、ゲーム・コントローラ、携帯アクセサリ、バッテリ、嗜好品等で使用されるものと同様のセキュア・エレメントをベースとするソリューションを採用するコネクテッド・デバイスが増え続けています。

Smart Things

- 資産管理
- eHealth（インターネット通信による健康管理など）
- 家電製品
- 消耗品機器
- ゲーム & アクセサリ

Smart Homes & Cities

- スマート・ビルディング
- ホーム・オートメーション
- 街路照明
- 都市交通
- エネルギーまたは水の供給
- ゴミ管理 & リサイクル

Smart Grid

- スマート・メータ
- コンセントレータ & ゲートウェイ

Smart Industry

- ネットワーク & サーバ
- 機械 & 生産設備
- コンピュータ

IoT分野におけるセキュリティの課題

ビジネスを保護：セキュアで信頼できる組込みシステムの構築

企業のIoTプラットフォームが信頼できるもので、考えられる脅威と脆弱性に対して保護されていることを保証するためには、アプリケーションの分野に関係なく、そのすべての主要コンポーネント、ネットワーク & クラウド、ゲートウェイ & コンセントレータ、およびSmart Thingsやノードが、セキュアな方法でデータを交換し通信できることが必要です。

IoTアプリケーションに対する脅威とその潜在的影響

デバイスの複製とデータ侵害：デバイス整合性に対する脅威

- 複製されたデバイスは直接的にOEMデバイスを、間接的にサービス・プロバイダの収益を毀損する
- 複製されたデバイスはデータ侵害とプライバシー損失に繋がる可能性がある
- セキュリティ侵害されたデバイスはサービス品質の問題と潜在的なサービス拒否を招く可能性がある

データ破壊：データ整合性に対する脅威

- データ破壊はサービス・レベルで誤った解釈を招く可能性がある（劣悪な意思決定の可能性がある）
- データ破壊はサービス品質を毀損し、プロバイダの評判とサービス品質に対するユーザの認識に影響を及ぼす可能性がある
- 極端な場合、データ破壊はサービス品質を毀損しユーザの安全に影響する可能性がある

データ侵害：データ機密性に対する脅威

- プライバシー侵害はユーザのプライバシーを毀損する可能性がある
- 盗まれたデータは最終的にサービス・プロバイダの責任に影響を及ぼす可能性がある
- 盗まれたデータはサービス・プロバイダの評判に影響を及ぼす可能性がある

セキュリティの脅威にどう対抗するか?

グローバルIoTソリューションのすべての要素の保護をうまく保証するには、システムの可用性を維持しながら、システムの整合性とそのデータの機密性に対する脅威に効果的に対抗する必要があります。

整合性 & 機密性の保証

システムの整合性とデータの機密性を保護するために、企業は以下を保証するセキュリティ・サービスと機能の実装が必要です。

- デバイスが正規品であることを認証を通して保証
- デバイスが侵害されていないことをセキュア・ブートおよびセキュア・ファームウェア・インストール & アップデート機能の使用によって、プラットフォームの整合性を検証することにより実現
- データがセキュアな方法で交換されていることをセキュア通信を用いて保証
- システム・シークレットがセキュアな方法でプロビジョニングされ保存

認証

デバイスの認識と真正性の検証

正当なデバイスのみがホスト・サーバに接続されることをどう保証するか?
IoTソリューションのすべてのコンポーネントの間で、セキュアな方法でデバイス認証を実施し検証する必要があります。
これにより、機密データやコマンドの漏洩に対する保護のためにデバイスまたはサーバの複製や偽造が防止されます。

通信

セキュアなデータ交換

通信を改ざんや盗聴からどう保護するか?
データ整合性検証およびデータ暗号化機能の実装を通してデータ交換をセキュア化し、データ破壊の防止が必要です。

プラットフォーム整合性

セキュアなコード実行

デバイスの機能が意図通りであることをどう確認するか?
セキュア・ブートおよびセキュア・ファームウェア・アップグレード・ソリューションは、デバイスが期待通りの機能を実行することを保証し、サービス・ネットワーク・アクセス破壊を防止します。

セキュア・プロビジョニングとセキュア・データ・ストレージ

セキュアなプロビジョニング & ストレージ

デバイス内の重要な資産がセキュリティ侵害されていないことをどう保証するか?
重要なデータは、セキュアな方法で安全に保存、使用、およびアクセスすることが必要です。
これらの重要なデータはセキュアな環境でプロビジョニングされる必要があります。

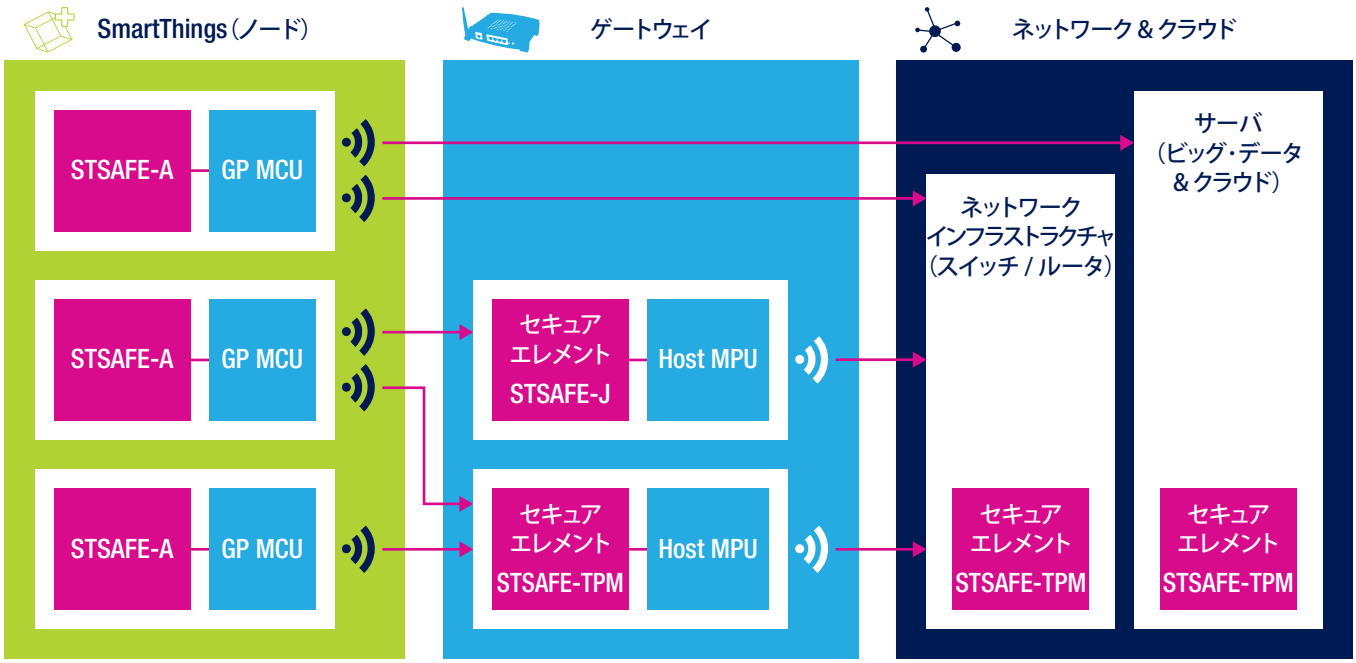
適切なレベルのセキュリティを備えたソリューションを実装できるかどうかは、IoTソリューション・プロバイダによるセキュリティ・ポリシーとリスク・アセスメント、および特定のアプリケーション領域(スマート・グリッド等)で要求される行政や市場の規制にかかっています。

製品ポートフォリオ

STSAFE™ファミリ：スケーラブルなセキュリティ製品

STSAFE™認証ソリューション

STSAFE製品は、IoTソリューションの3つの主要コンポーネントのセキュリティを保証するように設計されており、すべてが独立した第三者機関によって評価され、Common Criteria、BSI、FIPS、および固有の評価/検証方式を含むクラス最高のセキュリティ証明書を取得しています。



STのSTSAFE™セキュア・エレメント・ソリューション・ファミリは、最適化されたSTSAFE-Aソリューションから、柔軟性の高いSTSAFE-Jソリューション、STSAFE-TPMによるTCG準拠トラステッド・プラットフォーム・モジュール（TPM）ソリューションまで広範囲にわたります。

	STSAFE-A（最適化）	STSAFE-J（柔軟性）	STSAFE-TPM（標準化）
主な機能	認証、暗号化、署名、セキュア・ストレージ	• スマートグリッド・ソリューション用Enedis & BSIアプレット • オープン・プラットフォーム上のカスタム・アプレットのロード	プラットフォーム整合性測定 & レポート
プロビジョニング	• Sigfoxジェネリック部分 • 顧客固有のパーソナライゼーション：MOQ* = 50 Ku	• アプレットあり / なし	• ジェネリック部分 • 顧客固有のパーソナライゼーション: MOQ* = 1 Mu
ファームウェア	専用の暗号サービスを提供するネイティブOS	Java Card OS 3.0.4 Global Platform 2.1.1 CC EAL5+認証 BSI認証 Enedis準拠	TCG準拠OS TPM 1.2または2.0コマンド・セット CC EAL4+認証 FIPS 140-2認定
ファームウェア	セキュア・マイクロコントローラ セキュア・コアCPU/ROMまたはFlashメモリ、ハードウェア暗号アクセラレータ（RSA、ECC、DES、AESに対応）、CC EAL5+認証		

*MOQ：最小発注数量

エンド・ツー・エンドのセキュリティを実現するSTSAFE™

STは、組込みプラットフォームからゲートウェイやサーバまで、全範囲のIoTエコシステム製品に対応するセキュア・エレメントを提供しています。STSAFEセキュア・エレメントはデバイスの設計に統合され、その処理ユニットに接続されて、認証デバイスを補助し、プラットフォームの整合性とそのデータの機密性を保証します。

これらのすぐに使えるソリューションは、インク・カートリッジ等の消耗品内のスタンドアロン・チップとして、またはSTM32のようなアプリケーション・マイクロコントローラやマイクロプロセッサ（MPU）との組合せで使用することができます。

STSAFE-A（最適化）
- ブランド保護
- 資産管理
- スマート・シティ
- eHealth
- Industry 4.0

STSAFE-J（柔軟性）
- ユーティリティ
- ゲートウェイ
- スマート・シティ
- サーバ
- Industry 4.0

STSAFE-TPM（標準化）
- コンピュータ
- ゲートウェイ
- ネットワーク機器
- サーバ
- Industry 4.0

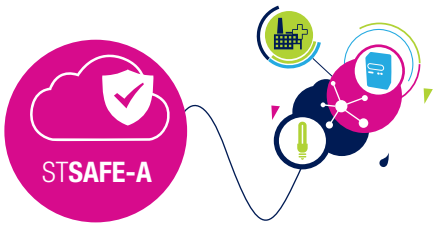
セキュアIoTソリューション用STSAFE™開発エコシステム

STは、ターンキー・ソリューションとソフトウェア・ライブラリおよびArduinoまたはSTM32 Nucleo準拠の開発ボードを含む開発ツール一式を備えた開発エコシステムを提供しています。これらのツールを使用することで、開発者は開発フェーズを大幅に簡易化し、コストと製品開発期間を削減できます。

出荷前の工場でのパーソナライゼーションにより、STのすぐに使えるSTSAFEソリューションは製品化を簡易にし、セキュリティを確保します。

STSAFE-A 最適化ソリューション

ビジネスを保護：セキュアで信頼できる組込みシステムの構築



STSAFE-Aは、Common Criteria EAL5+プラットフォーム上で動作する非常にセキュアな認証ソリューションで、そのセキュリティは第三者機関により認証を受けています。コマンド・セットは、厳密な認証への対応、TLSセッション用のセキュリティの高いチャネルの確立、署名の検証、セキュア・ストレージの提供、および使用状況監視のためのカウンタ減算用に設計されています。

IoTのためのセキュア・ターンキー・ソリューション

STSAFE-Aは、インク・カートリッジ、携帯やゲーム機のアクセサリ、USB Type-C™デバイス、Wi-Fi / Bluetooth® Low Energy (BLE) / 低消費電力広域ネットワーク (LPWAN) ベースのIoTデバイス、あるいは重要な証明書や高価値のサービスを運用するあらゆるIoTオブジェクト等のような詐欺や偽造に晒される脅威を持つアプリケーション向けに設計されており、自社ブランドを中心とするエコシステム構築の用途に最適なソリューションです。
STは、セキュア・マイクロコントローラに組み込まれた自社開発のセキュア・オペレーティング・システムから、ソリューションをアプリケーション環境に統合するためのサンプル・コードや、機密データを格納するためのパーソナライゼーション・サービスまで、広範囲の完全なソリューションを取り揃え、セキュア・システムの専門家とは限らないお客様のためにセキュリティ対策のシームレスな統合を提供しています。

特徴

- STSAFEセキュリティ機能
  - 認証
  - TLSセキュア・チャネル鍵確立
  - データ & 証明書ストレージ
  - 署名検証
- CC EAL5+ハードウェアを使用する最新式のセキュリティ
- LPWAN準拠LoRa & Sigfox
- USB Type-C™準拠

開発ツール

システム・オン・チップ
- ハードウェア
- 組込みソフトウェア
- 出荷時パーソナライゼーション

ホスト・ライブラリ
- 包括的なソフトウェア・ライブラリ一式

ツール & デモ・キット
- Nucleo拡張ボードとの互換性
- 包括的なソフトウェア・ライブラリ一式

利点

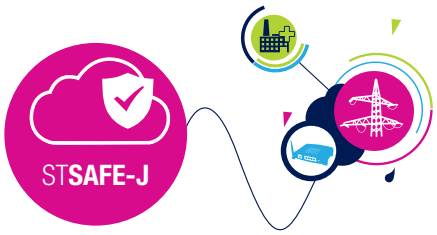
- セキュアOSとパーソナライゼーション・サービスを備えた完全なターンキー・ソリューション
- 小型プラットフォーム向けに最適化
- 標準マイクロコントローラと互換性のあるライブラリを使用して容易に統合可能

製品ポートフォリオ

品　名	OS 対応	インタフェース	認　証	パッケージ	動作温度範囲	NVM サイズ
STSAFE-A100	STSAFEセキュリティ	I²C	CC EAL5+ (HW)	SO8N (4x5mm) DFN8 (2x3mm)	-40 ~ +105°C	6KB
STSAFE-A1SX	Sigfoxネットワーク用 認証情報 & セキュリティ					
STSAFE-A110	• STSAFEセキュリティ • LoRa & Sigfoxネットワーク用パーソナライゼーション（オプション）					

STSAFE-J 高柔軟性ソリューション

柔軟性の高いJavaプラットフォーム



STSAFE-Jは、GlobalPlatform®、Java Card™ 3.0.4、および専用のJava Card™ モジュラー・アプリケーションをベースとする柔軟性の高いセキュア・ソリューションです。カスタム・アプリケーションの要件を満たす広範囲の暗号化およびセキュア・サービスを提供します。

さらに、Common Criteria EAL5+およびドイツのBSI認証により、スマートグリッド市場並びにコンセントレータ、ゲートウェイ、およびIoTデバイスに強力なセキュリティを必要とするアプリケーションに対応します。

認定保護プロファイルを備えたSTSAFE-J100

STSAFE-J100はコネクテッド・オブジェクト向け最新式セキュリティの提供に重点を置き、個々のオブジェクトに認証可能な書換えできないIDを与えます。また、暗号化通信を処理し、セキュア・ストレージを提供し、スマート・メータ、データ・コンセントレータ、ユーティリティ・ゲートウェイを含むIoTデバイスに容易に統合できます。STSAFE-J100セキュア・エレメントは、CC EAL5+認定ハードウェアとCC EAL5+認定セキュア・オペレーティング・システムを組み合わせており、市場固有のアプレットでカスタマイズ可能です。デバイスの設計者は、独自のセキュア・プロファイルを作成するか、またはスマート・ユーティリティ仕様（ドイツのBSIやフランスのEnedis）等のSTの認定取得済みプロファイルを利用して開発期間を短縮するかを自由に選ぶことができます。

お客様がSTSAFE-J100のフレキシビリティを十分に利用できるようにサポートし、脅威に対する保護を保証するために、STはセキュア・デバイス・パーソナライゼーション・サービスを提供しています。
個々のデバイスを固有のIDと暗号鍵でパーソナライズすることは、複製やハッキングへの耐性を備えた信頼できるハードウェアを作るためのセキュア・エレメントの基礎となる部分です。STのサービスは安全でコスト効率に優れ、セキュア・プログラミングに関するお客様の責任を軽くするとともに、プログラムされたデバイスの配布時に鍵とシークレットの漏洩を防止します。

開発ツール & サービス

開発者は、以下のような包括的な開発ツールとサービスのフルセットを利用できます。

- STM32 NucleoおよびArduinoボードとコンパチブルな拡張ボード
- アプリケーション・マイクロコントローラに組み込むためのサンプル・コードとライブラリ（認証、TLS）
- 信頼できるシークレットのストレージのパーソナライゼーション・サービス

特徴

- 柔軟性の高い暗号サービス（Java 3.0.4 + GP 2.1.1 + アプレット）
- CC EAL5+認証、BSI認証
- フランスのEnedis仕様に準拠

利点

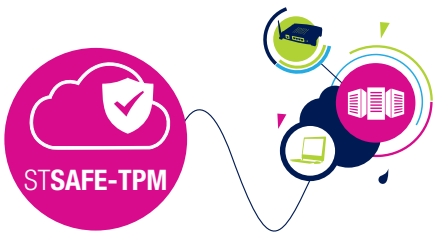
- 汎用的なSTのアプレットまたはお客様固有のアプレットによる柔軟性の高いJavaソリューション
- 認証による信頼できるネットワーク・アクセス
- セキュア・データ・ストレージ & セキュア通信
- パーソナライゼーション・サービス
- 拡張ボードとミドルウェア、開発エコシステム

製品ポートフォリオ

品　名	OS対応	インタフェース	認　証	パッケージ	動作温度範囲	NVMサイズ
STSAFE-J100	GP 2.1.1/JC 3.0.4	Contact ISO/IEC 7816 I²C	CC EAL5+	SO8N (6x5mm) DFN8 (4x4.2mm) VFQFPN32 (5x5mm)	-40 ~ +85°C	80KB
STSAFE-J100-BS	GP 2.1.1/JC 3.0.4 BSI Applet		CC EAL5+ BSI-DSZ-CC-1037-2018			17KB

STSAFE-TPM
標準化ソリューション

パーソナル・コンピューティングからコネクテッド・デバイスへ信頼性を拡張



コンピューティング・プラットフォームのセキュリティとユーザ資産の保護は、コネクテッド・デバイスを設計するOEMだけでなく、自分たちのプライバシーとデータの保護に関する懸念を強めているエンド・ユーザにとっても、非常に大きな課題となっています。
コネクテッド・コンスーマ・デバイスと産業用IoT機器の配備が増加していることで、この課題はさらに重要性を増しています。

STSAFE-TPMは、トラステッド・コンピューティングのための最も包括的でコスト効率に優れたシステム・オン・チップを提供する標準化されたセキュア・ソリューションです(Common CriteriaおよびFIPS認証取得済み)。

トラステッド・コンピューティングのための標準化された認証取得済みソリューション

コンピューティングは、もはや従来のパーソナル・コンピュータに限りません。今では、体系的にコネクティビティを統合した新しいタイプの機器を含む形で拡張しています。その結果、さらに、これらの新しい技術による普及率の高さも、新しいセキュリティ面での懸念を強調しています。

100以上の業界リーダーで構成された国際的な標準化団体であるトラステッド・コンピューティング・グループ(TCG)は、機器の整合性、健全度チェック、強力なユーザ認証、セキュア・ネットワーク・アクセス、データと資産の保護等のセキュリティ課題に対応するオープンな規格と仕様を提供しています。

STSAFE-TPM製品は、TCGのトラステッド・プラットフォーム・モジュール(TPM)仕様に完全準拠し、コンピュータ & IoTプロファイルをカバーしているだけでなく、Common Criteria EAL4+およびFIPS 140-2認証も取得しています。

このコスト効率に優れたシステム・オン・チップは様々なパッケージおよびインタフェースでの提供が可能なため、広範な接続型機器のための柔軟性の高いソリューションを提供します。STSAFE-TPM製品は広い産業用温度範囲での動作が認定されているため、市場で最も適切かつ包括的なTPM製品です。

特徴

- TPM 1.2 & TPM 2.0ライブラリ
- TPM 1.2 & TPM 2.0スイッチ機能
- TPMファームウェアのセキュア・フィールド・アップデート・モード
- Common Criteria(CC)EAL4+、TCG、およびFIPS 140-2認証
- Windows 10 Redstone(RS)認定
- Linux TPMドライバとコンパチブル
- 広い温度範囲 : -40°C / +105°C

利点

- ハイ・エンドのセキュア・マイクロコントローラがベース
- 認証取得済みのハードウェア・ベースの信頼のルート
- 大容量のセキュア・ユーザ不揮発性メモリ
- 独立認証局(CA)によりルート署名されたTPM証明書
- シームレスな実装(ISO/IEC 11889準拠)

製品ポートフォリオ

品　名	OS 対応	インタフェース	認　証	パッケージ	動作温度範囲	NVM サイズ
ST33TPHF2ESPI	TPM 1.2/TPM 2.0	TCG SPI	CC EAL4+/FIPS140-2/TCG1.2 & 2.0	TSSOP28 (9.7x4.4mm) VFQFPN32 (5x5mm)	-40 ~ +105°C	34KB
ST33TPHF20SPI	TPM 2.0		CC EAL4+/FIPS140-2/TCG 2.0			110KB
ST33TPHF2EI2C	TPM 1.2/TPM 2.0	TCG I²C	CC EAL4+/FIPS140-2/TCG1.2 & 2.0			34KB
ST33TPHF20I2C	TPM 2.0		CC EAL4+/FIPS140-2/TCG 2.0			110KB

life.augmented

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 052-259-2725

life.augmented

Order code: BRSTSAFE0918J

詳細はSTウェブサイトをご覧ください：www.st.com