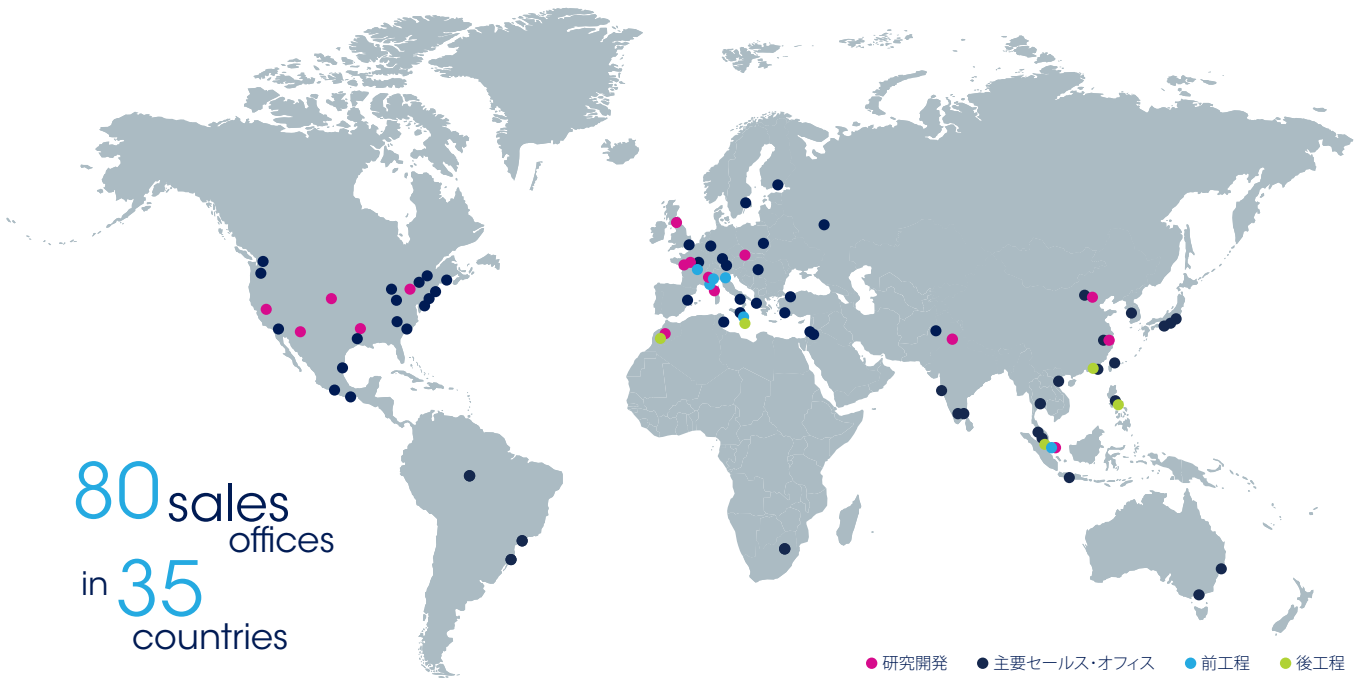
life.augmented

安全を保証する
セキュア・ソリューション

目次

STの概要

STは、私たちの暮らしに欠かすことのできないエレクトロニクス機器に、優れた性能と高い電力効率を特徴とした製品とソリューションを提供する世界的な総合半導体メーカーです。あらゆるシーンで活躍するSTの製品は、お客様が開発する次世代モバイルやIoT機器の他、よりスマートな自動車、工場、都市および住宅の実現に貢献します。
STは、生活をより豊かにする技術革新を通じ、「life.augmented」の実現に取り組んでいます。STは、10万社を超えるお客様に半導体を提供しており、2018年の売上は96.6億ドルでした。
さらに詳しい情報はSTのウェブサイトをご覧ください。http://www.st.com/jp



- グローバルな半導体企業
- ヨーロッパ最大の半導体メーカー
- 2018年の売上高は**96.6億**ドル

- 従業員数：約**4万6000**人
- 主要工場：**11**工場

- 世界各国に**80**のセールス＆マーケティングオフィス
- ニューヨーク証券取引所、パリ証券取引所、ミラノ証券取引所に上場

あらゆるシーンで活躍するST製品

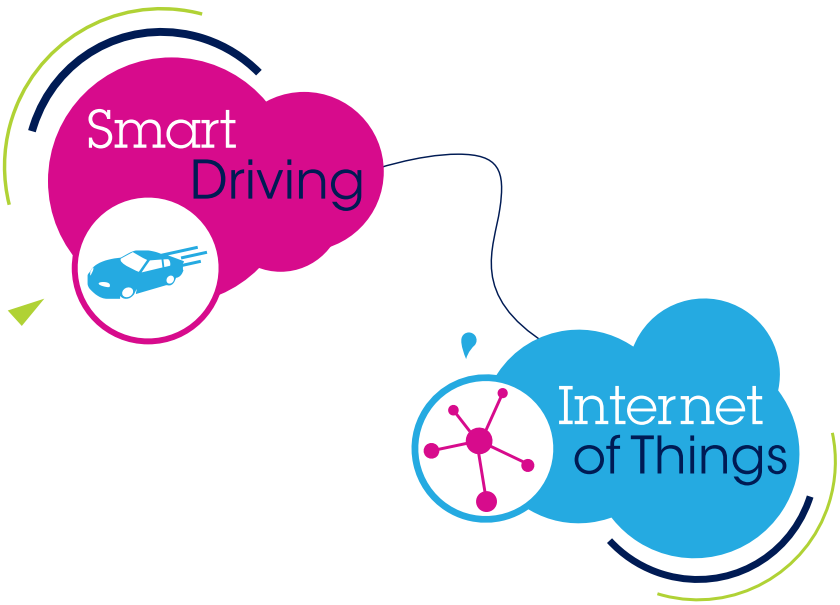
より安全で環境に優しく
接続性の高い**運転**を実現

住居および都市のスマート化
により生活の向上、セキュリ
ティの強化、および有効資源
の活用を実現

life.augmented

よりスマートで接続性が高く
環境認識が可能な
日常生活用品を実現

よりスマートで安全性が高く
効率的な工場や作業場を確保
するため**産業分野**の進化を実現

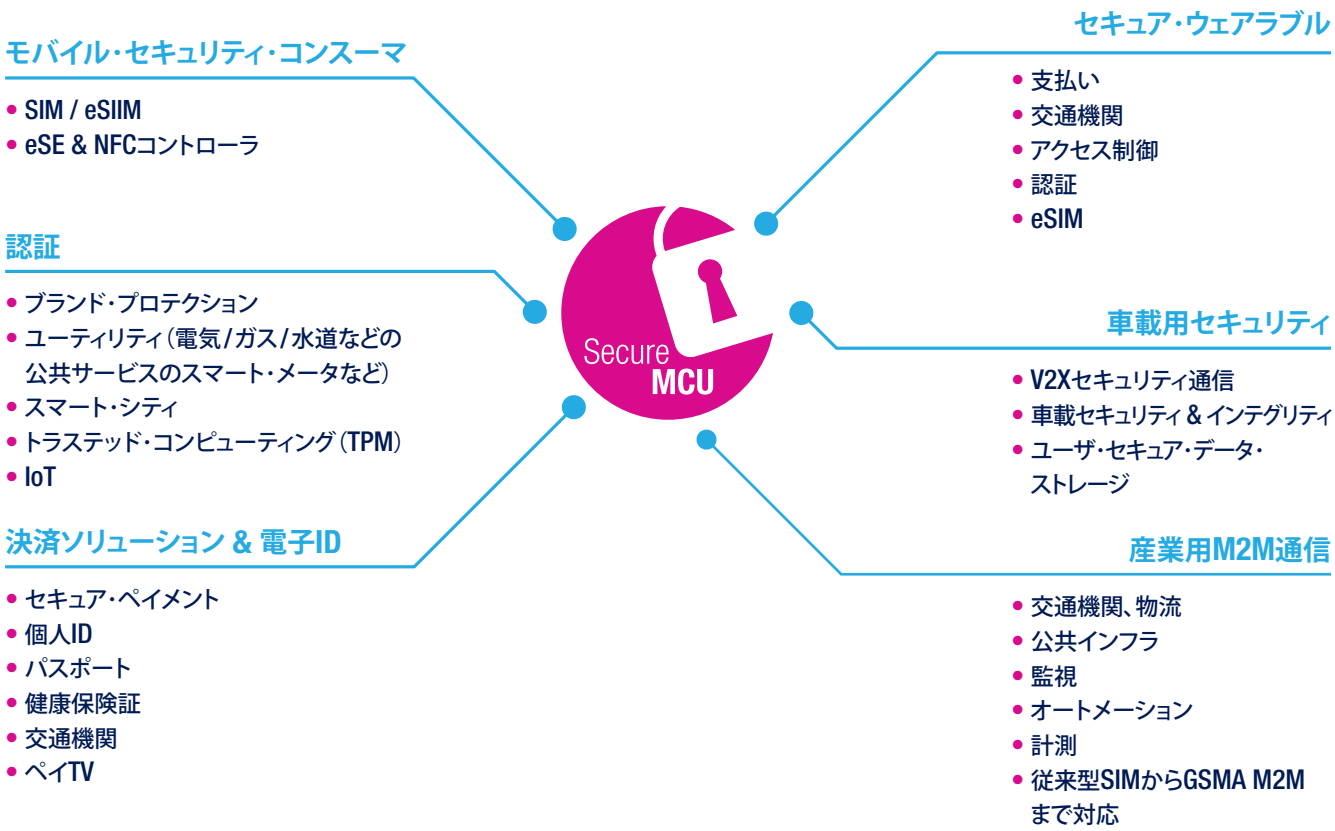


セキュア・アプリケーション

スマートカード技術をベースとするセキュア・アプリケーション市場は、1995年以来、銀行、ID、SIM、交通機関、およびペイTVなどのアプリケーションにより発展してきました。
コンスーマ機器の堅牢なセキュリティに対する需要の高まりと市場の進化に伴い、企業向けの公開鍵基盤（PKI）やトラステッド・プラットフォーム・モジュール（TPM）等のセキュア・ソリューションと、ブランド保護や盗用防止 / 偽造防止などの各メカニズムの提供により適用範囲が拡大しています。
組込みセキュア・エレメント、eSIMデバイス、M2Mデバイス、NFC対応デバイス、および非接触カードの導入により、携帯電話とワイヤレス技術が普及し、さらに進化しています。
将来は、モノのインターネット（IoT）による「つながる世界」で、スマート・グリッドやスマート・ホーム、スマート・シティ、自律走行車やスマート・ワールドなどの様々な領域においてセキュアに接続されたコネクテッド・デバイスを使用することにより、この技術のさらなる進化が予測されます。

STのセキュア・マイクロコントローラ

STのセキュア・マイクロコントローラとターンキー・セキュリティ・ソリューションは、急速に拡大しているコネクテッド・デジタル・ワールドにおいて、プライバシーを保護することで、より高い安心感を提供します。
SIM、バンキング、ID等の従来型スマートカード・アプリケーションから、セキュア・モバイル・トランザクションやIoT等の最新アプリケーションまで、STは最適なソリューションを提供することができます。
STのセキュア・マイクロコントローラは、最新のセキュリティ標準（Common Criteria、EMVCo、CUP）に従って認定され、ISO/IEC 7816、ISO/IEC 14443タイプA & B、NFC、USB、SPI、およびI^2Cを含む接触および非接触の両方の通信インタフェースを完全にカバーしています。
セキュア・マイクロコントローラに組み込まれたセキュア・オペレーティング・システムから、完全なイネーブルメント & パーソナライゼーション・サービスまで、完全なソリューションを提供することにより、STはセキュア・システムの専門家ではないお客様にもセキュリティ機能のシームレスな統合の実現をサポートします。



STのセキュア・マイクロコントローラ製品ポートフォリオは、主に以下のとおりです。

- バンキング & 電子IDソリューション：従来のスマートカード分野（決済、身分証明、交通機関、ペイTVなど）に対応
- セキュア・ウェアラブル：モバイル機器やウェアラブル機器によるセキュアな決済に対応
- コンスーマ・アプリケーション向けモバイル・セキュリティ：モバイル/ウェアラブル製品におけるセルラー・コネクティビティ用のSIM/eSIMソリューション、および近距離無線通信（NFC & eSE）用のセキュア・ソリューションに対応
- 認証：ブランド保護、TPM、IoTネットワーク用の高性能な認証ソリューションに対応
- 産業用マシン・トゥ・マシン（M2M）：IoT、産業機器、ネットワーク・インフラにおけるeSIMセキュア通信に対応
- セキュア・オートモーティブ：テレマティクス（eSIM/eSE）やゲートウェイ（eSE）におけるセキュリティに対応

バリュー・チェーン

バリュー・チェーン

サプライヤ

STは、多数のサプライヤおよび協力会社から、シリコン・インゴット、原材料、装置、電力、ガス、化学製品、およびサービスの提供を受けています。

研究開発の構想と設計

製品の開発は、アーキテクチャの構築、配線設計、電気的・論理的シミュレーション、チップ・レイアウト、およびシリコン・エッチング用マスク作成を含む複数の工程で構成されています。

製造前工程

チップの製造は、プレーン・シリコン・ウェハから始まり、数百から数千のダイのエッチングまで、約400の独立したステップからなる工程です。

電気的ウェハ・ソート(EWS)

シリコン・ウェハ上のダイを電気的にテストしています。この工程は、ウェハ・ソートまたはプローブと呼ばれます。セキュア・マイコンは、セキュアな環境下でHSM(ハードウェア・セキュリティ・モジュール)を使った組込みソフトウェア、キーおよびデータのプリローディングが必要です。

製造後工程(組立て & 最終テスト)

シリコン・ウェハをダイに切断し、パッケージに組立て格納します。その後、チップはテストされてからお客様に出荷されます。

セキュア・プリパーソナライゼーション

セキュア・マイコンは顧客固有のセキュリティ鍵やデータをセキュア環境下でロードします。

持続可能なテクノロジー

STは、原材料の採掘から生産終了まで製品寿命の前段階において、社会および環境資源の対する改善の取組みを進めています。

認証

STは、サプライ・チェーンにおいてRBA(Responsible Business Alliance : 責任ある企業同盟)の行動規範を遵守し、倫理、社会、環境、衛生および安全のリスクに対応するISO(International Organization for Standardization : 国際標準化機構)およびOHSAS(Occupational Health and Safety Assessment Series : 労働安全衛生マネジメントシステム)認証を義務付けています。また、RMI(Responsible Minerals Initiative : 責任ある鉱物イニシアティブ)に参加しています。

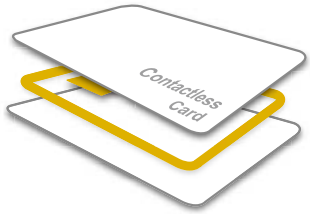
STは、品質、環境、安全性、およびセキュリティ上の規格適合および認定を確保できるように、製品の設計、製造、プリ・パーソナライゼーションを行っています。

- 継続マネージメント・システム
- ISO/TS 16949品質管理システム
- MasterCardカード品質管理(CQM)認定
- ISO 50001/ISO 14064環境管理規格
- Common Criteria EAL5+/EAL6+およびFIPS 140-2 セキュリティ評価
- ISO/IEC 15408コンピュータ・セキュリティ認定
- OHSAS労働安全衛生マネージメントシステム
- 事業継続マネージメント
- ISO 22301事業継続規格
- GSMA SAS-UP eUICCパーソナライゼーション・サイト認定

テクノロジー

非接触とNFC

ST31デュアル・インタフェース・セキュア・マイコンは、銀行、電子ID、交通系アプリケーション向けにセキュアで高速な非接触トランザクションを実現するように設計されています。STは携帯型機器またはウェアラブルでのNFCベースのソリューション向けに、NFCコントローラ・ファミリST21NFCから、ST31またはST33セキュア・エレメントとアクティブ・ロード・モジュレーションをベースとするboosted NFC対応STS392xブースタまたはNFCコントローラST21NFCを組み合わせたST53 / ST54システム・イン・パッケージ・プラットフォームまで、完全な製品ポートフォリオを提供しています。



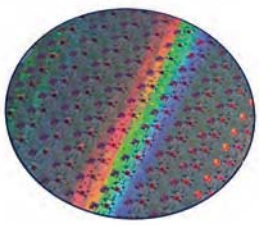
ISO/IEC 14443 Type A,B
ISO/IEC 18092

マルチ・プロトコル

様々なマルチプロトコルRFインタフェースに対応するST31セキュア・マイコンは、マルチアプリケーションで利用できる高い汎用性を特徴としています。ISO / IEC 14443タイプA、B、NFC、ISO / IEC 18092、および超高ビット・レート・プロトコルのすべてが利用可能で、自動検出モードによる適切なリーダ・プロトコルの自動的な検出とデバイスの動的な適応が可能です。ST21NFCおよびST54ファミリは、NFCのすべてのモード（リーダ / ライタ、カード・エミュレーション、ピア・ツー・ピア）を網羅しており、あらゆるNFCの使用法に対応します。

MIFARE®

MIFARE®アプリケーションを含むマルチアプリケーション・ソリューションに対応するオプションのセキュアMIFARE®ライブラリ（MIFARE Plus®およびMIFARE® DESFire® EV1 / EV2ライブラリ）がSTのプラットフォーム上で利用可能です。



Arm®コア・プロセッサ

Arm® SecurCore®プロセッサを内蔵したST31およびST33プラットフォームは、卓越した演算性能と、高速 / 高信頼性のトランザクションを可能にする低い動作時消費電力を実現しています。ソフトウェアの設計では、認知度の高いArm®開発環境と、クラス最高のコード密度のメリットを利用することができます。

Flashテクノロジー

STは先進技術の研究開発に継続的に投資しており、研究開発とデバイス製造のどちらも自社で行っています。最新のSTのセキュア・マイコンは40nm Flashテクノロジーをベースとし、高度な機能を備えた製品を最適化されたコストでお客様に提供することができます。

高い柔軟性

STのFlashテクノロジーにより、開発から製造まで、バリュー・チェーン全体で高い柔軟性を提供します。

- ROMマスク・サイクル・タイム回避により、製品開発期間の大幅な短縮
- 製造の最終段階でソフトウェアをロードすることにより、生産リード・タイムを短縮
- 在庫管理の最適化

性能と信頼性

高速プログラミング速度は、チェーン・モードで最大10µs/byteに達します。STのFlashテクノロジーは、ページ当り最大50万サイクルの消去/書込み操作と30年間のデータ保持という優れた耐久性と保持性能を特徴としています。

セキュリティ & 認証

1984年
マイコン・ベースのバンキング用スマートカードIC登場

2000年
ST19SF08が初のEAL4+ Common Criteria認証を取得

2007年
楕円曲線暗号 (ECC) ライブラリを備えたセキュアRFプラットフォームがEAL5+ Common Criteria認証

2010年
Flashテクノロジーと Arm® SecurCore® SC300プロセッサを集積化したST33

2012年
Arm® SecurCore® SC000プロセッサを備えた32bitマイコンST31がEAL5+ Common Criteria認証を取得

2016年
ST31がCUP（中国銀聯ユニオンペイ）に対応

2016年
IoT認証向けSTSAFEファミリをリリース

2017年
ST33J2M0がCommon Criteria & EMVCo認証、STSAFE-TPM 1.2 & 2.0 Common Criteria & TCG認証、STSAFE-J Common Criteria & BSI認証を取得

2018年
GSMA SAS-UP eUICCサイト認定を取得

セキュリティと認証

セキュリティ分野で30年以上の豊富な経験を持つSTの実績は、EMVCo、Visa、Mastercard、NFC、MTPS、China Union Pay、FIPSおよびCommon Criteria等の機関から授与された賞や認証により実証されています。
さらに、STはセキュア・マイコン・ソリューションに対して、電子部品メーカーとしては初となるeSIM製品向けGSMA SAS-UP認証を受け、STのセキュア・デバイスが高レベルのセキュリティを提供し、さまざまな市場に対応する柔軟性を備えていることを実証しました。
セキュアな製造チェーンを持つSTは、お客様にセキュア・ソリューションを提供できます。
また、STのセキュア・マイコン・ポートフォリオのセキュリティは、AESおよびKeccak暗号アルゴリズムの設計者でもあるSTの暗号専門家が持つ高レベルの専門性により保証されています。
接続機器の数が増えると、マルウェアや偽造ソフトウェアが特定の機器を制御したり、接続先ネットワークを制御 / 侵害する危険性も高まることになります。
そのため、OEM、ユーティリティ、およびネットワーク・プロバイダが、機器やネットワークのセキュリティにより、接続型機器の信頼性の強化を推し進めます。
接続機器に耐タンパー・セキュア・エレメントを追加することで、エンド・ユーザのプライバシーとデータ / IP / ブランド保護を保証する堅牢な認証、プラットフォーム完全性、および開発から製造・パーソナライゼーション工程にいたるまで高いセキュリティが提供されます。
セキュア・エレメントの標準的なターゲット・アプリケーションとして、プリンタ、コンピュータ、ゲートウェイやIoTエンドポイント、およびセンサがあります。


PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2017/50

ST33J2M0 A02

Développeur : STMicroelectronics

EAL5 Augmenté

Commanditaire : STMicroelectronics
Centre d'évaluation : Serma Safety & Security


Security Accreditation Scheme

Accredited Supplier

Certificate

This is to certify that

STMicroelectronics, Tao Payoh, Singapore

has participated in the GSM Association Security Accreditation Scheme for UICC Production (SAS-UP) and satisfied the scheme's requirements.

This certificate remains valid until the end of July 2019.

Secure MCU

安全を提供する STのセキュア・マイコン

セキュア・マイコン・ソリューションは、スマートカード技術、モバイル・セキュアな決済、セキュア接続ソリューションの急速な進歩に基づいて発展しています。

バンキング & 電子ID

バンキング、電子ID、ペイTV、交通機関向け ハードウェア & ソリューション

ST31
STPay

セキュア・ウェアラブル

非接触アプリケーション向け ハードウェア & ソリューション

ST31
ST53
ST54

コンスーマ向け モバイル・セキュリティ

モバイル・トランザクション（コンスーマ）向け ハードウェア & ソリューション

ST33 eSIM, eSE
ST21NFC
ST54

STは、次のような包括的なセキュリティ機能を提案しています。

- 自社テクノロジー
- ハードウェアおよびソフトウェア認定済みセキュリティ
- 暗号およびアーキテクチャに関する専門技術
- セキュア環境
- セキュリティ・コミュニティへの深い関与

IoT向け認証

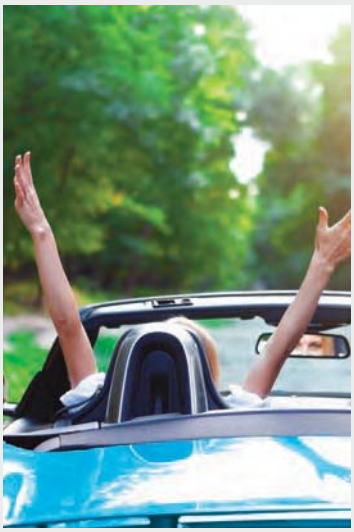
ブランド保護、コンピュータ、IoT向けソリューション

STSAFE-A
STSAFE-J
STSAFE-TPM

産業 & IoT用 M2M

M2M通信ソリューション向けハードウェア & ソリューション

ST32-M
ST33-M
M2M Solutions



セキュア オートモーティブ

コネクテッド・カー向けハードウェア & ソリューション

ST33-A eSIM, eSE
ST33-A TPM

決済ソリューション & 電子ID

STのバンキング・カード & 電子ID向け製品ファミリは、接触型、非接触型、接触・非接触デュアル・インタフェース（ISO/IEC 14443 Types A / B & ISO / IEC 18092）セキュア・マイクロコントローラの完全なポートフォリオを提供しており、従来型のスマート・カードから革新的なウェアラブル機器まで、広範囲のバンキングおよび電子IDアプリケーションを実現します。
STは、これまでにセキュア・マイクロコントローラをベースとする35億枚以上のバンキング・カードの販売実績があり、銀行業界において確固たる実績を持ち、金融系および交通機関向けカードに広く採用されています。

決済ソリューション & 電子IDソリューション

ST31セキュア・マイクロコントローラ・ファミリは、身分証明、ペイTV、交通機関、SDA/DDAバンキング・アプリケーション向けに設計されています。Arm® SecurCore® SC000プロセッサと非接触通信用に最適化されたアーキテクチャを備えたST31は、MIFARE Plus®、MIFARE Classic®、およびMIFARE DESFire®ライブラリなどの幅広いポートフォリオを提供します。このプラットフォームは、Common Criteria、EMVCo、中国銀聯ユニオンペイ（CUP）など、最高のセキュリティ規格に対応しています。
STのSTPayシステム・オン・チップ・ソリューションは、静的Java、動的Java、MULTOS OSベースのソリューションなどの即使用可能なバンキング・ソリューションを包括的に提供し、Visa、Mastercard、CUP、AMEX、Discover、JCB、CPAやその他多くの国内独自ブランドなどの幅広い決済アプリケーションに対応しています。
パーソナライゼーション・ラインの迅速なセットアップを実現するため、STPay製品は、Entrust Datacard（CPVプログラムの一部）などの主要なパーソナライゼーション機器サプライヤによって検証およびサポートされているEMV®カード・パーソナライゼーション仕様（CPS）に準拠し、MIFARE Classic®、MIFARE Plus®、MIFARE® DESFire®など、STの認定済みライブラリをサポートしています。

STPay : STのセキュア・ペイメント・ソリューション

- 主要ペイメント・アプリケーションに対応（Visa、MasterCard、JCB、American Express、Discover、Interac Flash等）
- 接触およびデュアル・インタフェース
- コモン・パーソナライゼーション・スタンダード準拠（CPS）
- Entrust Datacardカード・バリデーション・プログラム（CVP）
- MIFARE®およびMIFARE® DESFire®オプション

ST31

バンキング / ペイTV / 交通機関 / 身分証明アプリケーション

- 32bit Arm® SecurCore® SC000 CPU
- マルチプロトコル（ISO7816、ISO14443 A/B/F）
- EMVCo & Common Criteria認定

STPay

即使用可能なバンキング・ソリューション

- ST31セキュア・マイコン・ベース
- Java、Advantis、MULTOS OS
- 接触 & デュアル・インタフェース製品
- 交通機関アプリケーション専用のソリューション

セキュア・ウェアラブル

STのセキュリティ・プラットフォームは、決済、交通機関やさまざまな非接触処理など、ウェアラブル・アプリケーション向けの幅広い製品やソリューションを含み、セキュリティ認証、相互運用性、消費電力、集積化、最高のNFC性能などの課題に応えています。
STは、最適化したパッシブ型（バッテリ・レス）のST31セキュア・マイコンやSTPayソリューションから、セキュア・エレメントを集積した最先端のST53/ST54システム・イン・パッケージに基づく本格的なNFCソリューションまで、幅広いソリューションを提供しています。

新たな決済手段を可能にするboostedNFC™

STのboostedNFC™テクノロジーは、カード・エミュレーション機能を必要とする一方、過酷な環境で使用されたり、アンテナ用のスペースが限られるようなアプリケーションに最適です。STの高度なアナログ・フロントエンドであるSTS392xファミリは、アクティブ負荷変調テクノロジーを実装し、金属の多い通信が困難な環境にある場合や非常に小型のアンテナを必要とする場合でも、ウェアラブル機器における信頼性の高いNFC/非接触処理を実現します。

STPay-Boost & Fidesmo

STPay製品レンジは、STPay-I-Boostリファレンスの下でboostedNFC™テクノロジーを内蔵しています。STPay-BoostとFidesmoのパーソナライゼーションに基づき、STとFidesmoは、Kronaby製のスマート・ウォッチでセキュアな非接触決済を実現するターンキー・アクティブ・ソリューションを開発しています。

ST31

最適化されたパッシブ型

- 決済および交通機関向け
- Arm® SecurCore® SC000 CPU
- カード・エミュレーション、ISO14443 A/B/F
- MIFARE®
- クラス6アンテナまでサポート

ST53

最適化されたアクティブ型

- ハイエンド・マルチアプリケーション向け
- 決済および交通機関向け
- SEおよびRFブースタの統合
- カード・エミュレーション、ISO 14443タイプA
- MIFARE®
- クラス6以下

ST54

先進的なアクティブ型

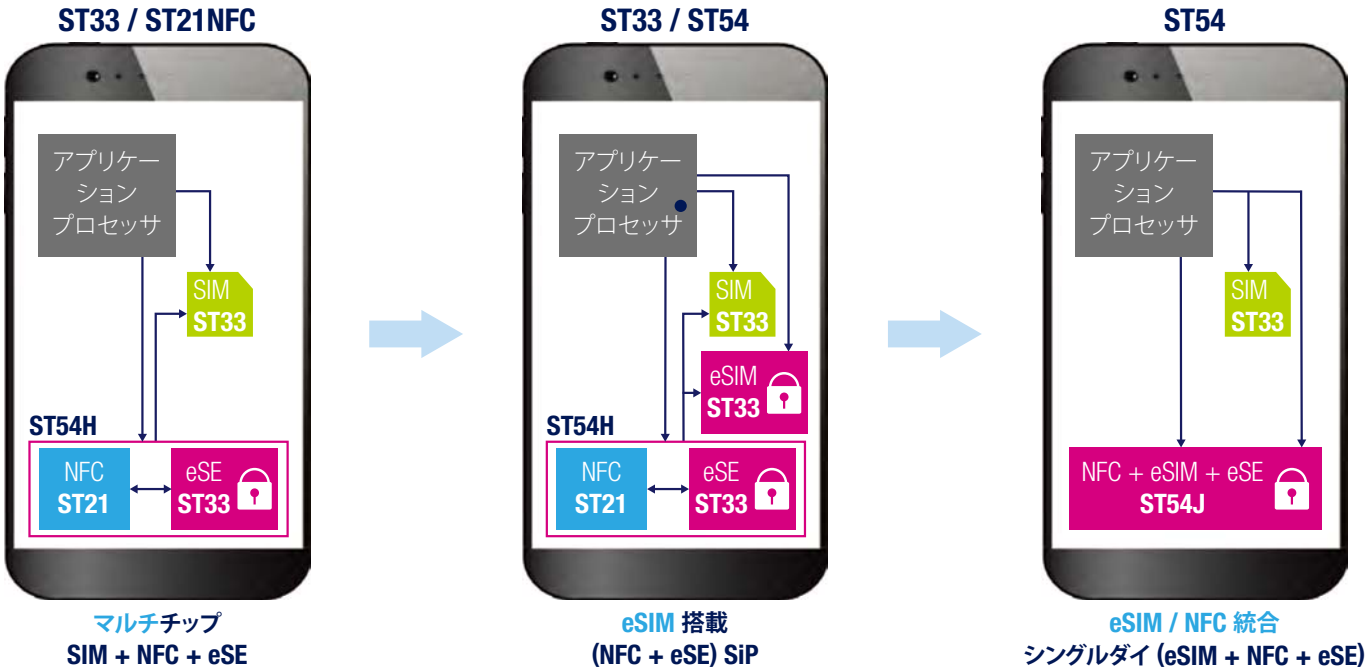
- SEおよびNFCコントローラの統合
- NFCカード・エミュレーション、ISO14443 A/B/F
- MIFARE4Mobile® v2
- 標準的アンテナ：100mm²未満、メタル・カバー

モバイル・セキュリティ・コンスーマ

モバイル・セキュリティ市場は、携帯電話に広く普及しているSIM技術から、スマートフォン、タブレット、ウェアラブル、ラップトップ機器などに幅広く普及しているNFC、組込みセキュア・エレメント（eSE）、および組込みSIM（eSIM）技術へと拡張しています。

効果的かつセキュアなモバイル・アプリケーションを構築するSTのソリューション

STは、最先端のNFCコントローラST21NFCから、広く導入されているST33セキュア・エレメントを集積したST54まで、幅広いNFCおよびeSE/eSIM製品やソリューションの提供により、セキュア・モバイル・トランザクション・アプリケーションのニーズに対応しています。



スタンドアロン・ソリューション

ST33 : eSIM/eSEアプリケーション向け

ST33セキュア・マイクロコントローラは、大容量のユーザFlashメモリを備え、組込みSIM、NFC-SIM、組込みNFCセキュア・エレメントなど、セキュア・アプリケーションの高度なセキュリティと性能の要件を満たします。
eSIMは、すでに主要なOEMによってタブレット、ウェアラブル機器、ノートPCに搭載され、引き続きスマートフォンにも広く導入されています。
eSIMは、基板に直接はんだ付けされる表面実装デバイスです。これにより、OEMは小型かつ薄型のモバイル機器の設計が可能になり、エンド・ユーザは選択したモバイル・ネットワーク事業者と契約できます。
eSIMデバイス内のSIMアプリケーションのリモート・プロビジョニングは、GSMAリモートSIMプロビジョニング仕様に準拠したサブスクリプション管理システムによって実現されます。
STのeSIMは、同種のパッケージの中で最も小型かつ薄型であるWLCSP（ウェハ・レベル・チップ・スケール・パッケージ）など、複数のフォーム・ファクタで提供されています。このデバイスは、GSMAリモートSIMプロビジョニング仕様に完全準拠し、主要なサブスクリプション管理プロバイダと完全に相互運用可能です。

GSMA SAS-UP認定

STは2018年、モバイル機器やコネクテッドIoT機器向けのeSIMをパーソナライズするためのGSMA認定をチップ・メーカーとして初めて取得し、追加のプログラミングなしで即使用可能なソリューションを提供しています。
通信認証情報によりカスタマイズされたeSIMは、小型化に加え、セキュリティ強化や柔軟性の向上を実現できます。

GSMA Security Accreditation Scheme　Accredited Supplier

ST21NFC : NFCコントローラ向け

非接触型モバイル・トランザクションの増加は、スマートフォンやウェアラブル機器などの民生用モバイル機器におけるNFCおよび組込みセキュア・エレメント（eSE）ソリューションの採用を促進しています。
タブレット、ゲーム機、ノートPC、ウルトラブックもNFC技術を搭載し、タグの読取りによるスマートIoT機器とのやり取りやクレジット・カードの承認が可能になっています。
ST21NFCDは、STの第4世代NFCコントローラです。高性能なRFブースタを内蔵し、最適なユーザ体験を実現するとともに、高度な相互運用性を確保して、OEMによる統合および認定作業をサポートしています。

モバイル・セキュリティを実現するeSIM/NFC統合ソリューション

ST54 : 高集積ソリューション向け

セキュア・モバイル・トランザクションの未来に対処するため、STはNFCコントローラST21NFCと実績あるST33セキュア・エレメントを組み合わせて、幅広いST54高集積ソリューションを提供しています。第1世代は、BGAパッケージで提供されるシステム・イン・パッケージ（ST54H）です。新しいST54Jシステム・オン・チップ（SoC）は、eSIM/NFC機能の融合化に対応するように最適化され、薄型WLCSPパッケージでシングル・チップとして提供されます。
ST54Jは、モバイル機器やIoT機器向けに高度な機能を組み込み、STのソフトウェア・パートナー・エコシステムも利用できるため、モバイル決済や電子チケット発券におけるよりスムーズなユーザ体験や、モバイル機器に複数の通信事業者を登録するより利便性の高いリモート・プロビジョニングを実現できます。

ST21NFC

NFCコントローラ

- 小型メタル・カバー・アンテナに対応
- 実装部品数の削減
- 低消費電力モード

ST33

eSE/eSIM

- GP2.2オペレーティング・システム
- 大容量ユーザ・メモリ
- MIFARE®
- DFN、WLCSP、またはNFCを備えたBGA

ST54

NFC & eSE/eSIM

- SEおよびNFCの統合
- マルチアプリケーションおよびNFC
- MIFARE®
- WLCSP、BGA

IoT向け認証ソリューション

企業のIoTプラットフォームの信頼性を確保し、可能性のある脅威や脆弱性からの保護を実現するには、アプリケーションの分野にかかわらず、あらゆる主要コンポーネント、ネットワークとクラウド、ゲートウェイやコンセントレータ、さまざまな電子端末やノードがセキュアにデータを交換し、通信できる必要があります。

IoTの市場とアプリケーション

最新のセキュア組込みシステムは、現在、広く導入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用のコネクテッド機器へと拡大しています。スマート・メータ、スマート・シティ、スマート・ホーム、そしてIndustry 4.0イニシアティブなどのスマート・インダストリで使用されるコネクテッド機器からのデータは、高い信頼性を確保する必要があります。ますます多くのコネクテッド機器において、プリンタ、PC、ゲーム・コントローラ、携帯電話のアクセサリ、バッテリ、各種の高級嗜好品に使用されているものと同様なセキュア・エレメントに基づくソリューションが採用されています。

STSAFE™ファミリ：スケーラブルなセキュリティ・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確保するように設計され、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認証を取得しています。

STSAFE-A（最適化タイプ）

- ブランド・プロテクション
- 資産管理
- 公共サービスなどのスマート・メータ
- スマート・シティ
- スマート・アグリカルチャ
- Industry 4.0
- Eヘルス（インターネット通信などによる医療情報の交換や遠隔治療）

STSAFE-J（柔軟性タイプ）

- 公共サービスなどのスマート・メータ
- ゲートウェイ
- スマート・シティ
- サーバー
- Industry 4.0

STSAFE-TPM（標準化タイプ）

- 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
- 公共サービスなどの機器
- その他あらゆるプラットフォーム

STSAFE™-A : 組込みシステム向けに最適化されたソリューション

STSAFE-Aは、インク・カートリッジ、携帯電話やゲーム機のアクセサリ、USB Type-C™機器、Wi-Fi/Bluetooth Low Energy (Bluetooth LE) /省電力広域ネットワーク (LPWAN) に基づくIoT機器、重要な認証情報や高価値のサービスを運用するIoTオブジェクトなど、不正行為や偽造のリスクがあるアプリケーション向けに設計され、自社ブランドを中心としたエコシステムの構築に最適なソリューションです。

STSAFE-A100オープン開発キット

- STSAFE-A100データシート
- STSAFE-A100 STM32 Nucleo拡張ボード (X-NUCLEO-STSA100)
- MorphoおよびArduinoコネクタ
- STSAFE-A100ソフトウェア・パッケージ (STSW-STSA100)
- ドライバおよびユース・ケース・サンプル

STのSTSAFE-A100評価ツール・セット (STSW-STSA100) は、充実したSTM32 Nucleoのエコシステムを拡張し、セキュアなIoT機器、医療用プローブやアクセサリなどの高価な消耗品、各種コンスーマ製品の開発を簡素化する再利用可能なソース・コードを活用してセキュア・エレメントの統合を促進します。この評価ツールは、www.st.com/stsafe-aでダウンロード可能です。

STSAFE™-J : Javaプラットフォームを備えた柔軟なソリューション

STSAFE-J100はコネクテッド・オブジェクトに対する最先端のセキュリティの提供に重点を置き、各オブジェクトに認証可能な書換えできないIDを付与します。機器の設計者は、カスタマイズ可能なアプレットの自由度を生かし、独自のセキュリティ・プロファイルを作成するか、またはドイツのBSIやフランスのEnedisなどのスマート・ユーティリティ仕様に対するSTの認定取得済みプロファイルを利用して製品開発期間を短縮できます。

STSAFE™-TPM : トラステッド・コンピューティング向け標準化ソリューション

STSAFE-TPM製品は、TCG (トラステッド・コンピューティング・グループ) の仕様に完全準拠し、コンピュータおよびIoTプロファイルに対応し、Common Criteria EAL4+およびFIPS 140-2認証も取得しています。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・チップを提供します。このコスト効率に優れたシステム・オン・チップは、さまざまなパッケージやインタフェースを提供し、幅広いコネクテッド機器に対応した柔軟性の高いソリューションを提供します。

アプリケーション

- コンスーマ製品
- 機密性の高い/高価な消耗品
- スマート・インダストリ & スマート・シティ
- ユーティリティ & ゲートウェイ
- コンピュータ
- ネットワーク機器 & サーバ
- IoTノード
- 資産管理

STSAFE-A

コネクテッド機器向けに最適化

- 認証およびTLSセキュア・キー確立
- CC EAL5+ハードウェアに基づく最先端のセキュリティ
- USB Type-C規格準拠
- LPWAN認証準拠
- 顧客のニーズに対するセキュア・パーソナライゼーション

STSAFE-J

ゲートウェイ向けの柔軟なプラットフォーム

- 柔軟な暗号サービス (Java 3.0.4 +GP 2.1.1 + アプレット)
- CC EAL5+、BSI認証
- 顧客のニーズに対するセキュア・パーソナライゼーション

STSAFE-TPM

標準化されたソリューション

- TPM 1.2 & TPM 2.0ライブラリとスイッチ機能
- TPMファームウェア用のセキュア・フィールド・アップグレード・モード
- CC EAL4+、TCG、FIPS 140-2認証

M2M産業 & IoT

コネクテッド機器は、リモート制御やリアルタイムの資産管理など、さまざまな重要な利点をもたらします。さらに、セルラー・コネクティビティの登場によって機器同士の接続が容易になり、多種多様な機器を追加することが可能となっています。そして、こうした新しい可能性に対処するには、従来とは異なる仕様が必要です。
STは、コネクティビティ製品のラインアップを多様化し、あらゆるセルラー・コネクティビティ・ソリューションに対応可能な幅広い製品を提案しています。

柔軟なセルラー・コネクティビティ・ソリューション

セルラー・コネクティビティには、異なる市場向けに設計された2つのタイプがあります。1つ目のタイプは従来型のSIMで、スマートIoT機器向けのセルラー・コネクティビティのみを含みます。導入が容易であるため、このタイプは迅速な製品化が可能です。2つ目の最新タイプは、GSMA SGP02仕様で規定された新しい組込みSIM（eSIM）です。これは、eSIM自体に影響を与えずにネットワーク・プロバイダ（プロファイル）の無線による変更を可能にするスケーラブルなソリューションです。eSIMは、柔軟かつコスト面で最適化されたソリューションです。

信頼性と高品質

環境に応じて、STは、セルラー・コネクティビティ・ソリューションに適合するM2M産業/IoTアプリケーション向け専用製品を提供しています。ローエンド・ソリューションは、ST32ファミリに基づき、シンプルかつ小型で迅速に統合できるスマートIoT製品を対象としています。この製品はSIMに対応しています。
産業機器に対応するため、STは高度なデータ保持機能と高い温度範囲を備えた過酷な環境条件をサポートするST33ベースのソリューションを提供しています。
さらに、ST33G1M2Mは、CC EAL5+およびGSMA M2M認証を取得しています。

ST32H

IoT用SIMソリューション向け

- シンプル & コンパクト
- 単一のセルラー・コネクティビティ（SIM）対応のJava Cardフレームワーク環境

ST32F-M

産業用SIMソリューション向け

- 産業用M2Mの堅牢性（50万サイクル、温度範囲：-40°C～+105°C）
- セルラー・コネクティビティ（SIM）

ST33-M

産業用eSIMソリューション向け

- eSIMによるスケーラブルな通信（GSMA M2M準拠）
- GSMA SAS-UP認定（HW & OS）
- 産業用M2Mの堅牢性

車載用セキュリティ

コネクテッド・カーが増加し、自動車業界が自動運転へのロードマップを描く中で、車載テレマティクス、ゲートウェイ、および電子制御ユニット（ECU）にセキュア・チップが搭載され始めています。
セキュリティはこうした新しい課題の核心であるため、STはセキュア・ソリューションの開発に取り組み、デジタル技術の新時代に向けて幅広い要件に対応しています。

コネクテッド・カー向け組込みセキュア・ソリューション

コネクテッド・カーのセキュア・エレメントと組込みSIMは、サービスの窃用、不正なネットワーク・アクセス、機器のクローン作成、偽造、データ盗聴、データ破壊から保護するための多数の重要機能を実現します。

- セキュアな車車間・路車間（V2X）通信：緊急通報、診断、ソフトウェア・アップグレード、決済 & インターネット・サービス、ADAS、その他機密性の高いサービスやシステム用
- 車内セキュリティ通信とプラットフォームの完全性確保
- ユーザ・データ・ストレージによる物理/サイバー攻撃の防止、乗客の安全性と自動車動作の保証、データ・プライバシーの確保

こうした課題に対処するため、STはST33G1M2Aを開発しました。ARM® SECURECORE® SC300 32BIT RISCコアをベースにしたST33G1M2Aセキュア・マイクロコントローラは、オートモーティブ・グレード・アプリケーション向けの高品質なセキュリティ・ソリューションを実現します。

ST33-A TPM

車載向けに標準化

- TPM 2.0サービス
- ユーザ・データ/セキュア・キー・ストレージ
- 車内通信のセキュリティと完全性

ST33-Aセキュア・エレメント

セキュア車載ソリューション

- ユーザ・データ/セキュア・キー・ストレージ
- 通信のセキュリティと完全性

ST33-A eSIM

セキュアな自動車用セルラー・コネクティビティ

- セルラー・コネクティビティ
- セキュアな通信
- 緊急通報システム（eCall）

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: BRSMCU0419J

詳細はSTウェブサイトをご覧ください：www.st.com