



# 脚光を浴びる IoT セキュリティ

IoT ビジネスの成功を後押しするセキュリティ・ソリューションの提案

[www.infineon.com/loT-security](http://www.infineon.com/loT-security)

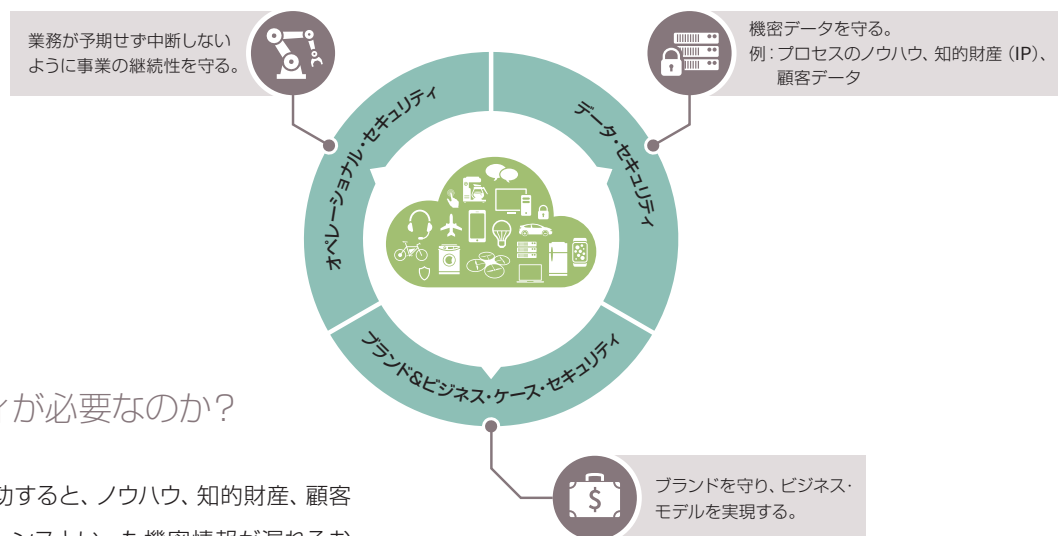


# 明るい IoT セキュリティに向けて

## IoT セキュリティへの不安

モノのインターネット (IoT) やマシン・ツー・マシン (M2M) 通信の普及は、ネットワーク化されたデバイスや装置の増加を意味します。小さな家電から、大規模通信ネットワークや複雑な産業オートメーション・システムまで、多くが専用の組み込みコンピューティング・システムによって制御されています。

ネットワーク化の流れが加速し続けるにつれ、ユーザの利便性と快適性が高まるのに加えて、企業には新しいビジネスやサービスのモデルがもたらされています。しかし、組み込み分野のセキュリティは、大きく遅れがちです。攻撃対象が広がるにつれて、セキュリティ上の脆弱性が飛躍的に高まり、秘密データや知的財産 (IP) を守り、改ざんなどを防ぐことが難しくなります。



## なぜ IoT セキュリティが必要なのか？

組み込みシステムへの攻撃が成功すると、ノウハウ、知的財産、顧客データ、プロセス・インテリジェンスといった機密情報が漏れるおそれがあります。また、攻撃によって業務が中断すれば、事業の継続性を損ない、企業のブランド・イメージや業績、存続そのものを危険にさらします。

## 課題

- › より巧妙で強力になってゆくハッカーの攻撃からシステムを守る。
- › 守りたい資産の価値と予算の制約とをバランスさせる。
- › 確実に信頼できる、実装可能なセキュリティ機能を見つける。
- › 使いやすさを犠牲にせずに、システムのセキュリティを向上させる。

## 目的

- › 新しいビジネスやサービスのモデルを開発する。
- › イメージしやすく競争力のある差別化を考える。
- › パートナーのノウハウを活用することで、セキュリティへの投資を削減する。
- › サプライチェーン全体の管理を改善し、生産工場の選択の幅を高める。





## 提案

インフィニオンは、IoT セキュリティの課題に対応するために、実装が簡単で、スケーラブルかつカスタマイズが可能なターンキー・ソリューションの OPTIGA™ を提供しています。信頼できるアドバイザーとして、インフィニオンが複雑さや実装コストの削減をお手伝いします。セキュリティのノウハウやインフラストラクチャへ投資するよりも、ハードウェア方式のセキュリティ・ソリューションについて豊富な実績を持つインフィニオンの専門知識をご活用下さい。



## 脅威への防御

ソフトウェアは比較的容易に読み出して、複製や配布ができるため、それだけでは組み込みシステムを守るのに不十分です。データとプログラムを確実に保管し、外部からの不正操作を検出し、安全な保管や処理のためにデータを暗号化するには、セキュアなハードウェアが必要です。信頼の基点「ルート・オブ・トラスト」を設けて組み込みソフトウェアを信頼できるものにするために、ハードウェア方式を採用したインフィニオンのソリューションをご活用下さい。

OPTIGA™ は、セキュリティ上重要な三つの基本機能をサポートして、ルート・オブ・トラストを実現します。

### ＞ 認証

OPTIGA™ セキュリティ IC は、許可された人や機器の間でのみ情報が交換されるように、人や機器の認証を行います。

### ＞ 暗号化

セキュリティ・モジュールが暗号化や、秘密鍵の安全な保管を行い、秘密情報を守ります。

### ＞ 完全性

セキュリティ・チップがプラットフォームや装置、機器の完全性をチェックし、改ざんの特定制と不正変更の検出を行います。

セキュリティ・アーキテクチャー上にルート・オブ・トラストを設けるハードウェア方式のソリューションは、IoT の可能性を最大限に活かせる安心感を全ての人に与え、消費者や企業へ莫大な恩恵をもたらします。





## セキュリティを支える取組み

セキュリティ分野で 30 年の実績を持つインフィニオンの取組みは、明確かつ確実なセキュリティ製品で、お客様を支援することだけではありません。

インフィニオンは、製品のセキュリティ面以外の数々の点でも、信頼を得ています。第一には、工程のセキュリティを重視していることです。セキュリティ認定を取得した設計施設、生体アクセス制御を採用した専用のセキュリティ設備、そして何よりも、鍵のプログラミングを保護するセキュアな生産体制を整えています。

第二には、セキュリティ・エキスパートが、最新製品を厳しくテストしています。新しい攻撃手法を、継続的に製品コンセプトへ反映させ、製品のライフサイクルを適切に保っています。

さらには、開発や製造の工程と同様に、第三者認定を受けた製品ということです。多くのインフィニオン製品が、ドイツ当局による厳格なコモン・クライテリア認定に合格しています。

これらの取組みは、インフィニオンのお客様が、その先のお客様の信頼を得るための明快な説明材料になります。

# マーケットの広がり

セキュリティはニーズが複雑になるほど多様化します。基礎的な単純機能である認証ソリューションから、先進的なプラットフォームの完全性チェックのための堅牢な認定セキュリティ・モジュールまで、幅広い市場分野にわたる個々のセキュリティ・ニーズをサポートするために、業界最大の製品ラインアップを揃えました。

## IoT セキュリティ

### スマート・ホームセキュリティ

エアコンのセンサーから家全体の制御システムまで、あらゆるものの保護を可能にします。

- ▶ スマート・ホームのゲートウェイとサーバー間の通信をセキュアにする。
- ▶ ホーム・オートメーション機器を認証する。
- ▶ 偽のホーム・オートメーション機器から保護する。

実績のあるセキュリティ機能を使って、安全に新しいアプリケーションを使った新しいビジネスやサービスのモデルを創出し、全ての事業に柔軟性とコスト削減をもたらすことで、今日のスマート・ホームを魅力あるものにします。

### カーセキュリティ

ユーザの秘密データを守り、自動車をより安全にします。

- ▶ テレマティクス・システムの通信をセキュアに行う。
- ▶ インフォテインメント・システムを認証し、サービスを有効にする。
- ▶ リモート・メンテナンスの情報やファームウェアのアップデートをセキュアに行う。

インフィニオンは、自動車分野での長年の経験と豊富なセキュリティのノウハウを活かした最適なセキュリティ・ソリューションで、コネクテッド・カーを実現します。新しいビジネスやサービスのモデルを見つけるチャンスです。



# クラウド

## ICT セキュリティ

スケーラブルな製品ラインアップが、小型ネットワーク・スイッチから大規模ネットワークまで、あらゆる通信とアクセスを保護します。

- ▶ ネットワーク機器間のセキュアな通信によりデータを保護する。
- ▶ ソフトウェアのアップデートをセキュアに行い、ソフトウェアを保護する。
- ▶ ルーターで管理されたネットワーク・アクセスによって機器の完全性をチェックする。

ICT 分野での信頼されるパートナーとして、インフィニオンは幅広いパートナー・ネットワークを通じた実装やデバイス管理のサポートを提供しますので、最新セキュリティ・ソリューションを容易に導入頂くことができますので、お客様は優位性を保つことができます。信頼できるセキュリティ・ソリューションにより、新しいビジネスやサービスのモデルを創出できます。

## 産業セキュリティ

装置のセンサーから制御システムまで、あらゆるものをセキュアにし、製造業の長期的な成功をお手伝いします。

- ▶ オートメーション・システムと IT プラットフォーム間の通信をセキュアにし、秘密データと知的財産を守る。
- ▶ オートメーション・ネットワーク内のセンサーや機器を認証する。
- ▶ ソフトウェアやファームウェアのアップデートをセキュアに行い、知的財産を守り、操業の中断を防ぐ。

産業とセキュリティを融合する専門性と、個々の要件を満たすスケーラブルな製品ラインアップが、現代的なスマート工場を実現します。確立されたセキュリティのノウハウとインフラストラクチャを利用することで、セキュリティへの投資を抑制できます。





# 主なユース・ケース

多様な実績のある製品ラインナップにより、インフィニオン製品は考えられるあらゆるユース・ケース・シナリオへ対応可能です。オーダーメイドで行われる提案の最も代表的なシナリオを以下に紹介します。



## 機器の認証

ネットワーク上のユーザ、コンピュータ、機器や装置を識別し、許可された人や不正操作されていない機器にアクセスを限定する処理が認証です。ハードウェア方式のセキュリティでは、機器の認証情報（暗号鍵やパスワード）にセキュアな保管場所を提供して認証をサポートすることができます。クラウド、サーバー、その他の機器に接続しようとする機器やシステムのセキュアな認証を可能にするため、ハードウェア機器内にルート・オブ・トラストを設ける OPTIGA™ には幅広い製品ラインアップがございます。



## ブート・プロセスと機器の完全性の保護

組み込み機器をセキュアにするには、機器の完全性を保護して不正な変更を防ぐ必要があります。この際に重要なのは、機器のブート・プロセスを保護するという点です。セキュアなブート、ペリファイド・ブート、トラステッド・ブートとも呼ばれるブート・アクセス・プロテクションは、コンピュータ機器の不正ブートをブロックし、感染デバイスが IoT を通じてデータを送ることを阻止します。インフィニオンは、ブートの保護を強化し、完全性メトリクス管理の簡易化のため、OPTIGA™ ファミリーで多様なセキュリティ IC を提供しています。



## セキュアな通信

一般的な組み込みシステム・アーキテクチャでは、様々な規格や独自プロトコルを採用した異なるネットワークを経由して、機器とシステムが接続されます。例えば、傍受やメッセージの改ざんから通信を保護するには、システム間をセキュアにしなければなりません。OPTIGA™ は、暗号処理をサポートするだけでなく、通信プロトコルで使用される鍵や証明書を保管することで、セキュアな通信を可能にします。



## ソフトウェアやファームウェアのセキュアなアップデート

組み込みシステムのソフトウェアやファームウェアは、定期的なアップデートが必要です。しかしながら、アップデート中のシステムだけでなく、ソフトウェアそのものを保護することは容易ではありません。ソフトウェアだけで保護されるアップデートでは、一般に、ソフトウェアを読み出し、解析して、アップデートやシステムに侵入できるように変更されるリスクがあります。しかし、セキュアなハードウェアと組み合わせることで、ソフトウェアを信用できるものにできます。セキュアなハードウェア OPTIGA™ は、暗号化、異常および不正操作の検出、コードやデータのセキュアな保管により、コードの実行や保管を保護します。



## セキュアなデータ保護

組み込みデバイスには、秘密のユーザ・データが保管されている場合があります。このデータの機密性は、暗号化とセキュアな場所への保管によって保護できます。暗号鍵をセキュアに保管できるかが課題です。攻撃者が鍵を読み出せば、データを容易に復号化できてしまいます。OPTIGA™ は、データを暗号化し、暗号鍵をセキュアに保管することにより、この課題を克服します。

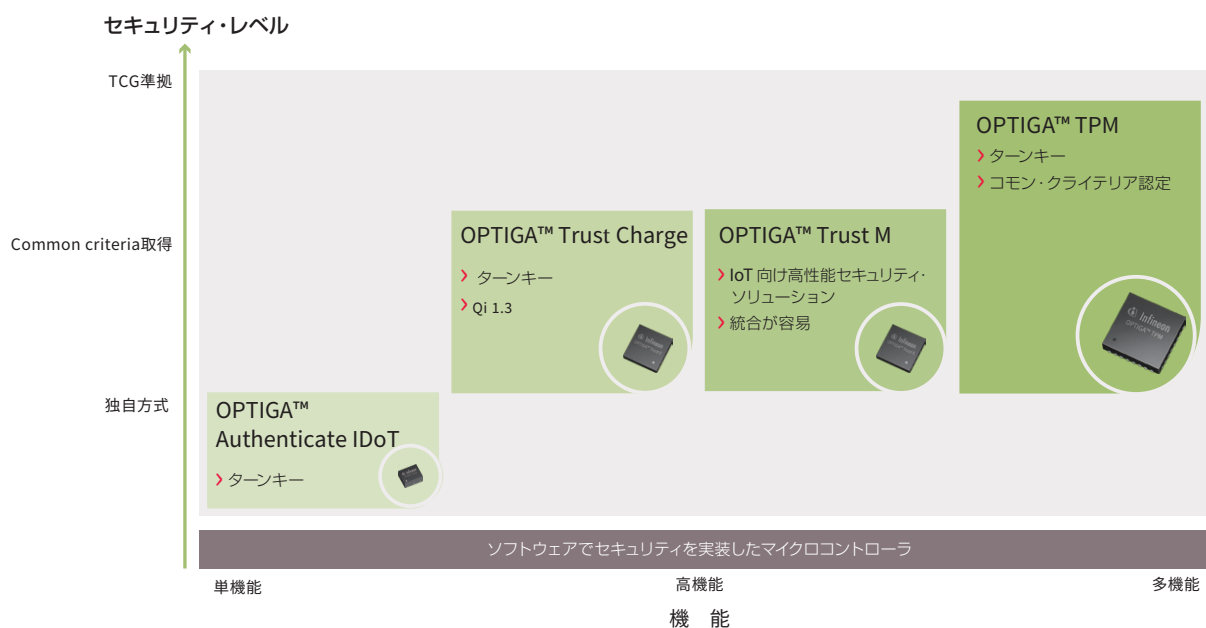




## セキュリティの課題に応える OPTIGA™

セキュリティ・ソリューション OPTIGA™ は、組み込みシステムへ簡単に実装できるよう設計されています。このハードウェア方式のセキュリティ・ソリューションは、お客様ごとの様々なニーズに対応できるように、単純な認証から、複雑なものまで複数あり、

最大の投資効果が得られます。OPTIGA™ ファミリーにより、信頼と実績の IoT セキュリティを実現します。



# 「OPTIGA™」ファミリー

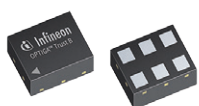
## 組み込みシステムのためのトラスト・アンカー

ターンキーもしくはプログラマブルなソリューションであるOPTIGA™ファミリーは、ビジネス・モデル、製造ノウハウやIPの保護に最適なレベルのセキュリティを提供すると同時に、

簡単に、簡単に実装できる特徴があります。OPTIGA™ファミリーは、偽造や模造、意図的な攻撃や思わぬ誤操作から組み込みシステムを守ります。

## OPTIGA™ Authenticate IDoT

### セキュリティの強化とシステム・コスト削減に向けた認証ソリューション



OPTIGA™ Authenticate IDoTは、信頼できる認証機能を簡単に実装したい組み込みシステムに向けた、強固な暗号ソリューションです。このセキュリティ・ソリューションは、純正品の信ぴょう性や完全性、安全性を守りたいシステム・メーカーやデバイス・メーカー向けに設計されています。このターンキー・ソリューションは優れた模造品対策となるため、OEM が純正品の信ぴょう性を維持し、ブランドやビジネスモデルを守る助けとなります。

#### 主な機能

- › 4つのECC認証モード（一方向、相互、ホストバイディング、ホストサポート）に対応
- › ロック（保護）可能な3種類の不揮発性メモリーサイズ（1K、2K、5Kbit）
- › 2つの標準温度オプション（-40～+85℃ / -40～+105℃、特別な-40～+120℃）
- › 2 ECC 163ビットおよび193ビット ODC
- › 2つのシリアル通信オプション（SWI & I2C + GPO）
- › 独立した不活性化構造を持つ安全なライフサイクル デクリメントカウンター
- › 設定可能なGPOオートトリガー
- › 設定可能なユーザーNVMロック

#### 主な機能

- › 低コストのシングル・チップ・ソリューション
- › 非対称暗号とチップ個別の鍵による高いセキュリティ
- › 開発が容易なターンキー・デザイン

#### アプリケーション

- › バッテリー認証
- › IoT 子機
- › 家電アクセサリ
- › IP および PCB 設計の保護
- › 純正交換部品
- › 医療および診断機器



# OPTIGA™ Trust Charge

## ワイヤレス充電向けの信頼性の高い認証ソリューション



インフィニオンのOPTIGA™ Trust Chargeは、Qi1.3のワイヤレス充電規格による電磁誘導方式ワイヤレス充電向けにセキュアなデバイス認証を提供する新しいターンキーソリューションです。OPTIGA™ Trust Chargeを使用したセキュアな認証は、偽物の充電器から民生機器やユーザーを守り、安全性をもたらします。

### 主な機能

- › WPC Qi 1.3認証
- › コモンクライテリア (Common Criteria) EAL6+ (high) 認証ドウェア
- › ECDSA P-256認証
- › NIST P-256, SHA-2 暗号化
- › Up to 10kBユーザーメモリー
- › Qi 認証方式
- › PKI
- › I2Cシリアル通信
- › USON10-2 パッケージ (3 x 3mm)
- › 対応温度範囲の広い製品も利用可能
- › フルターンキーソリューションには、ソフトウェアライブラリー、組み込み済みの証明書およびキーペアが含まれます

### 主なアプリケーション

- › 携帯電話
- › タブレット
- › カメラ
- › Qi 規格準拠の充電可能なアクセサリや小型のパーソナル電子機器
- › ヘルスケアテクノロジー機器



# OPTIGA™ Trust M

## IoT セキュリティに向けて最適化されたソリューション



OPTIGA™ Trust Mは、産業用オートメーション・システム、スマート・ホーム、家電機器、医療機器に向けたターンキー・セキュリティ・ソリューションです。この高性能セキュリティ・モジュールは、高性能のセキュリティを自社資産に簡単かつリーズナブルに導入できるように、システム側の実装をフルにサポートしています。自社の機器にOPTIGA™ Trust Mを実装すると、ブランドとビジネス・ケースを守り、競合他社から自社製品を差別化して、サイバー攻撃に対してより強固になります。自社の機器で正規品、完全性、機密性を保護するために必要とされる、相互認証、セキュアな通信、データ・ストアの保護、ライフサイクル管理、セキュアなアップデート、プラットフォーム完全性の保護など、広い範囲のユース・ケースに対応しています。

### 主な機能

- › 高性能セキュリティ・モジュール
- › ターンキー ソリューション
- › システム側の統合をフルにサポート
- › 暗号化ツール・ボックス
- › 標準動作温度モデル（-25～85℃）と拡張動作温度モデル（-40～105℃）を用意
- › USON-10 パッケージ（3 x 3mm）

### 主な特長

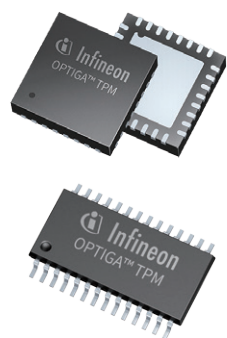
- › ネットワーク化される機器（IoT）向けのセキュリティ強化
- › 実装が容易
- › リーズナブルな導入
- › 新しい機能やビジネス・モデルの有効化

### アプリケーション

- › 産業用制御機器、自動化機器
- › 家電製品
- › スマート・ホーム
- › 医療機器

# OPTIGA™ TPM

## 標準化された高機能セキュリティ・ソリューション



TPM (トラステッド・プラットフォーム・モジュール) は、組み込みネットワークでのデバイスやシステムの整合性と信ぴょう性を保護する、標準化されたセキュリティ・モジュールです。実績ある TPM 1.2 や最新規格 TPM 2.0 への対応により、OPTIGA™ TPM は、鍵や証明書、パスワード用のセキュア・ストレージに加えて、専用の鍵管理機能を取り入れています。あらゆるニーズに応えるため、トラステッド・コンピューティング・グループ (TCG) 規格に基づいて認定された多彩な OPTIGA™ TPM があります。

### 主な機能

- › ハードウェアで実現された先進の暗号アルゴリズム (2048 ビット RSA 暗号、256 ビット楕円曲線暗号、SHA-256 など) を持つ高性能セキュリティ・モジュール
- › コモン・クライテリア EAL 4+ および FIPS セキュリティ認定
- › SPI、I2C、LPC インターフェイスのサポートによる柔軟な実装
- › 様々なアプリケーションに使える拡張動作温度モデル (−40 ~85°C)
- › 幅広いオープン・ソースのサポート

### 主な特長

- › 規格化されたシステムのため低リスク
- › 短期間での市場投入が可能
- › 優れた鍵管理をはじめとする幅広いセキュリティ機能による柔軟性
- › コンピュータ・プラットフォームへの実装が容易

### アプリケーション

- › PC および組み込み用コンピュータ
- › ネットワーク機器
- › 産業用制御システム
- › ホーム・セキュリティ、ホーム・オートメーション
- › 発送電システム
- › 自動車用エレクトロニクス

## 「OPTIGA™ TPM」ファミリー概要

SLB 9645	SLB 9660	SLB 9665	SLB 9670	SLB 9670
<ul style="list-style-type: none"><li>› TPM 1.2</li><li>› I2Cインターフェイス</li><li>› コモンクライテリア EAL 4+ 認定</li></ul>	<ul style="list-style-type: none"><li>› TPM 1.2</li><li>› LPCインターフェイス</li><li>› TCG およびコモン・クライテリアEAL4+ 認定</li><li>› FIPS 140-2 認定</li></ul>	<ul style="list-style-type: none"><li>› TPM 2.0</li><li>› LPCインターフェイス</li><li>› TCG およびコモン・クライテリアEAL4+ 認定</li><li>› FIPS 140-2 認定</li></ul>	<ul style="list-style-type: none"><li>› TPM 1.2</li><li>› SPIインターフェイス</li><li>› TCG およびコモン・クライテリアEAL4+ 認定</li><li>› FIPS 140-2 認定</li></ul>	<ul style="list-style-type: none"><li>› TPM 2.0</li><li>› SPIインターフェイス</li><li>› TCG およびコモン・クライテリアEAL4+ 認定</li><li>› FIPS 140-2 認定</li></ul>





# なぜセキュリティが必要なのか？

セキュリティは、事業上の必須要素から、事業上の優位性を得る要素へと進化してきています。適切に導入すれば、競争上、本物の差別化要因となります。

- ▶ セキュリティによってビジネス・モデルや IP を保護することができ、例えば、偽造品、不正操作によるアップデート、データの盗難などが原因の、サービスの中断や品質上の問題を回避しやすくなります。その結果、ブランドへの信頼や評判を築くことになり、成長と収益性の後押しとなります。
- ▶ 認定を受けたセキュリティ機能によって円滑で予測可能な操業が約束されることで、新しいビジネス・モデルを導入する道筋をつけることさえ可能です。
- ▶ 最新のセキュリティ機能によって計画外のダウンタイムをなくすことで、導入コストの節約と、収益への貢献が可能になります。

# なぜハードウェア方式のセキュリティが必要なのか？

ハードウェア方式のセキュリティ・ソリューションは、専用の保護された機能を備えていることで、ソフトウェアのみによるアプローチを性能面で明確に上回っています。さらに、認定を受けたハードウェア・ソリューションでは、独立機関による評価が追加して認められるので、ソリューション実現までの時間が短縮されます。ディスクリット・ソリューションでは、強固な改ざん防止、拡張性、動的なイノベーション・サイクルが実現されるだけでなく、実装も容易

になります。これは、セキュアな生産体制を必要としないなど、設計と生産の複雑さを低減できるためです。各種の規格に準拠した最高レベルのセキュリティを顧客に提供するために、専用のインフラストラクチャや専門家のノウハウに投資する必要がないため、ディスクリット・ソリューションの導入はコストの削減につながります。

# なぜインフィニオンを選ぶのか？

インフィニオンは30年以上にわたって、セキュリティ市場の先駆者であり続けてきました。毎年20億個を超えるセキュリティ・モジュール IC を出荷していることが、長年にわたってお客様の期待に応え、それを上回る専門知識、経験、問題解決能力を持っていることの確証となっています。インフィニオンは、研究開発と品質に強くコミットし、幅広いエコシステムにわたって多様なサポートと

パートナーのネットワークを築いています。それらに加えて、産業界に積極的に関わることで、インフィニオンは幅広い産業界にわたって選ばれるパートナーとなっています。今日のセキュリティに関する課題の複雑さを解消し、便利さと実装の易しさを兼ね備えたソリューションの構築をインフィニオンはお手伝いします。



モバイル版カタログ  
iOS および Android 向けアプリ

[www.infineon.com/security](http://www.infineon.com/security)  
[www.infineon.com/loT-security](http://www.infineon.com/loT-security)

インフィニオン テクノロジーズ ジャパン 株式会社  
[www.infineon.com/jp](http://www.infineon.com/jp)

© 2020 Infineon Technologies AG.  
All rights reserved.

Document number: B189-I0281-V3-5A00-JP-EC-P  
Date: 06 / 2020

**Please note!**

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

**Additional information**

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office ([www.infineon.com](http://www.infineon.com)).

**Warnings**

Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.