パナソニック株式会社
〒571-8501 大阪府門真市大字門真1006番地

2020年1月30日

IoT機器および産業機器の重要データを保護する多機能セキュアICを開発

【要旨】

パナソニック株式会社　インダストリアルソリューションズ社（以下、パナソニック）は、日々、高度化するセキュリティー対策を担う多機能セキュアICを開発し、2020年2月よりサンプル出荷を開始します。本製品は独自のセキュリティー機能を有し、IoT機器や工場などで使用される産業機器に追加実装するだけで機器の安全性を向上します。

【効果】

昨今、さまざまな分野において機器のIoT化が加速し、高度多様化するセキュリティー攻撃への対策が求められています。従来は認証鍵をICの外から書き込み、IC内に保有し続けていました。本製品はIC内部で固有の認証鍵を生成・保有、使用後に消去することで鍵の抜き取りをブロックし、重要データを強固に保護します。また、無線インターフェース機能のNFC［1］や放射線耐性が高いメモリー（ReRAM［2］）を搭載しているため、インターネット未接続機器や医療機器などへの適用が可能です。さらに機器の使用中だけでなく、製造から廃棄または再利用までのライフサイクル全体にわたって安全性の確保が可能となり、安心安全なIoT社会の実現に貢献します。

【特長】

1. IC内部で固有の認証鍵を都度生成・消去し、データのセキュリティー耐性を向上

2. 無線インターフェース機能のNFCと放射線耐性が高いReRAMを搭載

3. トラストサービス事業者［3］などと連携し、機器のライフサイクル全体にわたる安全性を向上

【従来例】

機器の認証鍵をIC外部から内部のメモリーに書き込み、メモリー内に保存していたため、認証鍵を抜き取られるリスクがあり、お客様側での安全な環境構築が必要でした。また、データが抜き取られたり改ざんされるリスクもありました。

【用途】

・IoT機器や産業機器全般（物流、スマート工場、ネットワーク機器など）
・放射線滅菌処理が必要な医療機器や医薬品の管理

【お問い合わせ先】

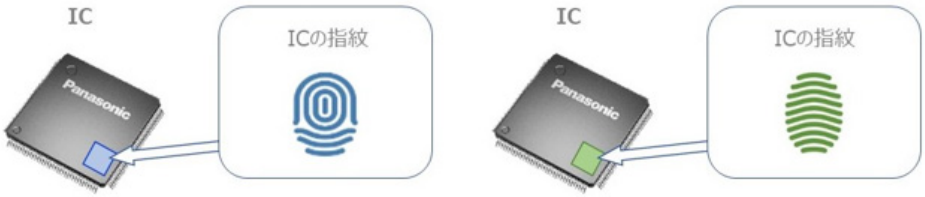
パナソニック セミコンダクターソリューションズ株式会社
https://www.panasonic.com/jp/company/pscs/contact.html?ad=press20200130

【特長】

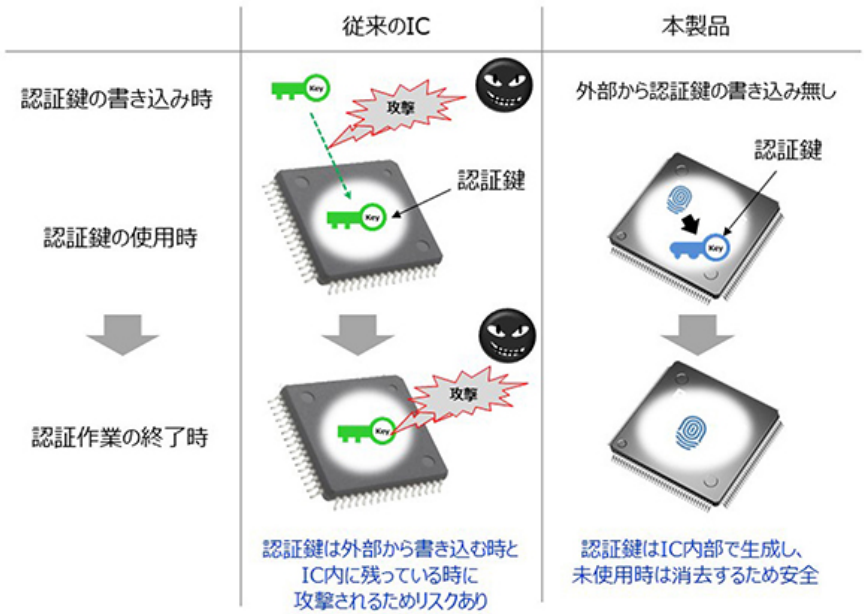
1. IC内部で固有の認証鍵を都度生成･消去し、データのセキュリティー耐性を向上

本製品は、独自のセキュリティー機能としてICごとに異なるアナログ情報を保有しています。このアナログ情報は人間の生体情報（指紋）のように一つ一つ異なります（ICの指紋）。このICの指紋はアナログ情報のため、コピーすることはできません。
本製品では、ICの指紋から固有の認証鍵を生成し、この認証鍵でメモリー内の大切なデータを暗号化しておくため、メモリー内のデータの抜き取りや改ざんへの耐性が向上します。
また、機器を認証する時にもICの指紋から認証鍵を生成し、認証作業が終了した段階で認証鍵を消去するため、セキュリティー耐性が大幅に向上します。

〔ICの指紋は一つ一つ異なる〕



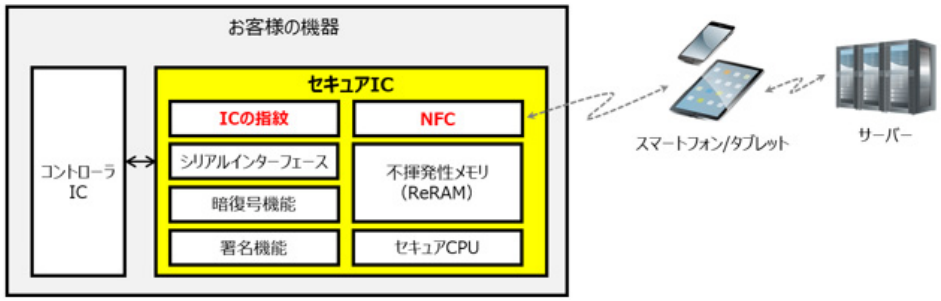
〔ICの指紋から認証鍵を生成し、認証作業の終了時は消去するため安全〕



2. 無線インターフェース機能のNFCと放射線耐性が高いReRAMを搭載

本製品には、無線通信するためのNFCを搭載しており、インターネットに接続されていない機器であってもスマートフォンやタブレット端末経由でインターネットに接続できます。それによってサーバーを利用した機器の相互認証が可能となり、なりすましなどを防止できます。また、エナジーハーベスティング機能[4]を使うことで、機器の電源がオフの状態であっても、NFCを介して機器内のコントローラICの情報やセキュリティーインシデントの記録などをスマートフォンやタブレットで読み取ったり、機器の動作設定を行うことができるため、システムの保守管理の容易化やユーザビリティー向上に貢献します。

〔NFCの利用例〕



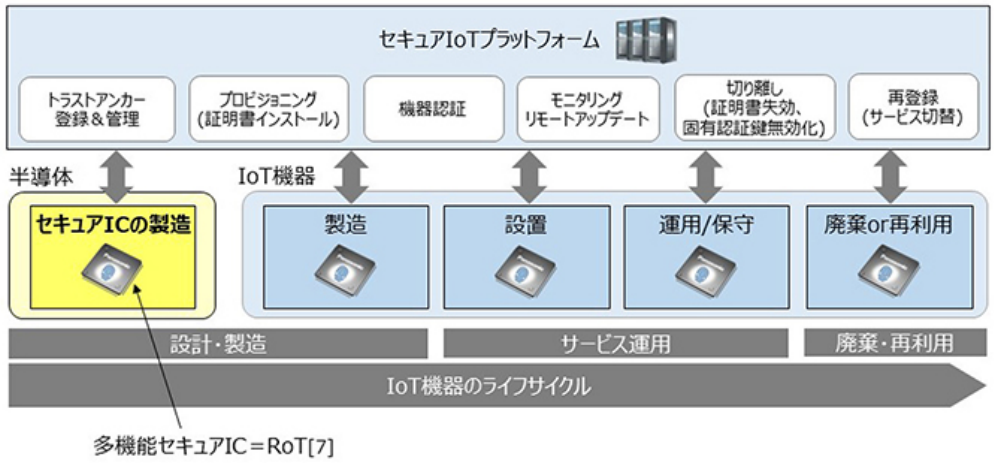
また、放射線耐性が高い不揮発性メモリーのReRAMを搭載しているため、放射線滅菌処理が必要な医療機器や医薬品の管理などへの適用が可能です。

3. トラストサービス事業者などと連携し、機器のライフサイクル全体にわたる安全性を向上

本製品は、トラストサービス事業者*などのセキュアIoTプラットフォームと連携する機能を搭載しています。そのため、トラストアンカー[5]を保有した本製品をIoT機器に組み込み、証明書による認証を実行することで機器の製造から廃棄または再利用までのライフサイクル全体にわたって安全性の確保が可能となり、安心安全なIoT社会の実現に貢献します。また、これにより、IEC62443[6]で定める制御システムに関するセキュリティー基準への適応が容易になります。

* 2020年1月30日現在、サイバートラスト社（代表取締役社長：眞柄 泰利）と開発連携の可能性を検討中。

〔本製品を利用したIoT機器のライフサイクル全体にわたる安全性確保例〕



【製品仕様】

セキュアIC(品番：MN67S3C0シリーズ)		
製造プロセス		40nm混載ReRAM
CPUコア	ARM SC000	Max. 40MHz
インターフェース	SPI	2ch（Single/Quad×1ch＋Single×1ch） Max. 40Mbps
	I2C	Fast mode（400kbps）
	NFC	ISO/IEC 14443 Type A ISO/IEC 14443 Type B JISX6319-4 FeliCa (注)
メモリ	ReRAM memory	256 KB
	RAM	16 KB
暗号（共通鍵）	DES	鍵長112
	AES	鍵長128/192/256
暗号（公開鍵）	RSA	鍵長1024/2048/3072/4096
	ECC	鍵長160/224/256/521
HASH		SHA-1/SHA-2
CC認証(ハードウェア)		EAL5+

注）FeliCaは、ソニー株式会社が開発した非接触ICカードの技術方式で、ソニー株式会社の登録商標です。

【用語説明】

［1］NFC

Near Field Communicationの略称で、国際標準化機構（ISO）が規定した近距離無線通信規格。

［2］ReRAM

Resistive Random Access Memory（抵抗変化型不揮発性メモリー）の略称で、金属酸化物薄膜にパルス電圧を加えることで大きな抵抗変化を生じさせ“0”“1"を記憶する。金属酸化物を電極ではさんだシンプルな構造で、製造プロセスが簡単であり、低消費電力特性や高速書き換え特性などの優れた特長を有する。

［3］トラストサービス事業者

IoTサービスにおけるトラストサービス事業者とは、IoT機器が本物であることや利用者の本人確認による真正性の確保、データの改ざん検知などによる完全性の確保などを行い、システムの有効性を担保する基盤となる仕組みを提供する事業者を指す。

［4］エナジーハーベスティング機能

太陽光や照明光、機械の発する振動、熱などのエネルギー（エナジー）を採取（ハーベスティング）して電力を得る技術で、ここではNFC機能を搭載したタブレットやスマートフォンが発する電磁波から電力を得る機能を指す。

［5］トラストアンカー

ここでは電子証明書に利用する情報（固有の認証鍵やID情報）を指し、この情報をRoTに保管することで電子的な認証を行うための信頼の基点となる。

［6］IEC62443

国際電気標準会議（IEC）が規定した、制御システムに関するセキュリティーマネジメントシステムの基準。

［7］RoT

Root of Trustの略称で、ここでは固有の認証鍵や電子証明書などの重要情報を保管するセキュアICを指す。

以上