# インフィニオン セキュリティ パートナー ネットワーク (ISPN)

セキュリティ
パートナー
プリファード

**パートナー ユースケース**

# 産業用システムでのIoT端末向け サーバー側管理システム

本システムは、多彩なIoT機器を柔軟にシステムに組み込むことができるオープン標準を利用し、迅速な製品化を実現するソリューションとして、Trusted Computing Group（TCG）の技術を利用したシステムです。

## 製品

OPTIGA™


www.infineon.com/ispn

# ユースケース

**アプリケーション・コンテキストおよびセキュリティ要件**

産業用システムでは、複数ベンダーの複数デバイスを同じネットワーク環境で管理します。Insight社は、TPM 2.0 (Trusted Platform Module)、内製のTPMソフトウェアスタック (TSS - TPM 2.0 Library)、測定ベースセキュアブート、OpalなどのTCG (Trusted Computing Group) 技術を利用して、オープン標準に準拠し、複数IoTデバイスを柔軟にシステムに適用させ、迅速な製品化を実現するターンキー・ソリューションとして、産業用システムでの複数IoT端末向けサーバー側管理システムを提供しています。

**課題**

産業用システムが外部ネットワーク (インターネット) に接続されると、ネットワークは世界中からの脅威にさらされます。ネットワーク全体にセキュリティを組込み、全デバイスの管理を可能にすることは、こうした脅威からシステムを保護するのに不可欠です。

**実装**

本システムはサーバーを使用してエンドポイントの完全性を検証し、安全にエンドポイントを使用できるようにします。 サーバーの検証が完了しないかぎり、エンドポイントは必要なアプリケーションを実行しません。 サーバーは、独自の完全性検証を実行します。 Opalドライブは、ディスク盗難時のデータ保護に役立ちます。

**ユーザーにとってのメリット：**

ユーザーは次のような仕組みを利用できます。

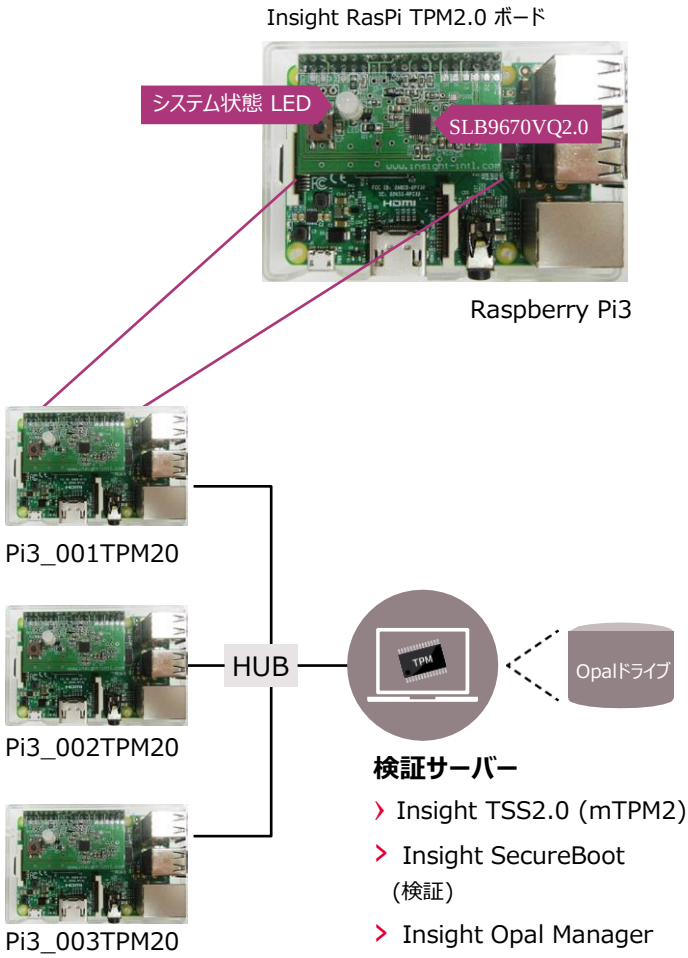
- いつでも安全にエンドポイントを使用できます。
- ステータスLEDを確認することで、エンドポイントの正常性状態が分かります。
- サーバー自体のセキュリティを確認し、ディスクの盗難からファイルを保護します。

# ソリューション

本システムは、TCG（Trusted Computing Group）の信頼の起点 (Root of Trust) テクノロジーを使用することにより、セキュリティ保護された環境で暗号化機能を実行できます。機能要件は、TCG準拠のTPM 2.0、Opalドライブ、およびそれらを操作するソフトウェアです。

本システムでは、インフィニオンの OPTIGA™ TPM SLB 9670 (TPM バージョン2.0) がセキュリティ面で重要な役割を果たしています。世界中の数百万もの PCや組込み機器が、OPTIGA™ TPM によって様々なサイバーセキュリティの脅威から保護されています。

## 2017 TCG JRF TPM2.0 デモシステム




**Insight RasPi TPM2.0 ボード**

- Raspberry Pi 2 およびPi 3に対応
- Linuxで動作
- Insight TSS2.0(mTPM2)
- Insight SecureBoot (Hash値に基づく)

**検証サーバー**

- Insight TSS2.0 (mTPM2)
- Insight SecureBoot (検証)
- Insight Opal Manager

1. 各Raspberry Pi 3を起動します。
2. Insight SecureBootでハッシュ値の計測を行います。
3. Insight SecureBoot 検証を使い、サーバーのホワイトリストに基づき PCR値(SLB9670) の検証を行います。
4. 一致した場合、RasPi3の緑色のLEDを点灯し、一致しなかった場合は、赤色のLEDを点滅させます。また、データが改ざんされた場合には、Insight SecureBootでリカバリエンジンを始動し、Opal ドライブから「正しいファイル」を回復させます。
5. Pi 3の起動が正常に完了した後、Insight Enc/Decを開始し、TSS2.0 (mTPM2)を使用してTPMに署名をします。

# ソリューション

**インフィニオンのOPTIGA™TPM SLB 9670 2.0の特長**

- TCG, EAL, FIPS 140-2 , その他多くの認証を取得済み
- エンドポイント起動時のファイルの測定値の保存
- 最新の暗号化エンジンによる暗号化/復号化、乱数生成

本ソフトウェアには、Insightが提供する測定ベースのセキュアブート、TPM 2.0ライブラリ、Opal Managerが含まれます。

**Insight TPM 2.0ライブラリの機能**

- HMAC計算機能がインストール済み
- セッション (復号化、暗号化、監査) 機能をサポート
- 広範な組合せ試験を実施済み

さらに、Insightは、暗号化/復号化および鍵の複製を利用したTPMアプリケーションの開発しやすさを考えて設計されたTAW (TPM Access Wrapper) を提供しています。

**メカニズム**

この操作のメカニズムは、エンドポイントが起動されたときにセキュアブートソフトウェアを使用し、ハッシュ（SHA 256）でエンドポイントファイルを測定することによって行われます。 測定結果は、Infineon OPTIGA™TPMに保存されます。 保存された値をサーバー内のホワイトリストと比較し、問題がなければ通常動作を実行します。 同時に、ステータスLEDの確認により、エンドポイントの正常性状態が確認できます。 サーバーの安全性については、サーバー自体も測定ベースのセキュアなブートを実行します。 サーバーにはTCG Opalドライブが搭載されており、ディスクを盗難から守り、暗号化によりファイルを保護します。Opalは、ファイル保存用で、ネットワークからのファイル盗難を防ぐためのセキュリティ機能用の領域を使用します。

# パートナー

インフィニオン セキュリティ パートナー ネットワークのパートナーは、お客様のビジネスを揺るがせかねない脅威を理解し、ビジネスを守るためのソリューションを提案・構築し、実装します。 インフィニオンは、システムセキュリティに対する能力と、強固で信頼性の高いセキュリティソリューションを設計・提供できるかどうかに基づき、パートナーを選んでいます。パートナーのビジネス内容は、セキュリティコンサルティング、セキュリティソリューションの提供、電子設計、システムインテグレーション、トラストサービス管理など多岐にわたっています。そのうちのいくつかは市販品ですが、それ以外のものはカスタム品です。

**インサイトインターナショナル株式会社**

インサイトインターナショナル株式会社は、TPM (Trusted Platform Module) に対応したTSS (TCG Software Stack) ソフトウェア開発を行っています。TPM 1.2および2.0に対応したTCGソフトウェアスタック (TSS) 、計測に基づくセキュアブートソフトウェア、Opal管理ソフトウェアを提供しており、マーケットのTPM要求に10年以上対応してきた実績があります。インサイトインターナショナル株式会社の事業内容は、複合機 (MFP)、POS、ネットワーク端末などの幅広いアプリケーションを対象とした組込みシステム市場にも及んでいます。

インサイトインターナショナル株式会社は、業界をリードする企業と提携し、顧客がより手ごろな価格で製品を製造し、最新の業界基準に対応できるよう高性能なソフトを提供しています。

インサイトインターナショナル株式会社は、1984年、東京に本社を設立。2009年には、最初のTPM1.2用TSSを出荷。2017年にインサイトインターナショナル株式会社は、TPM2.0用TSSをリリース・出荷し、近く世界中の顧客にも提供することを計画しています。

**インサイトインターナショナル株式会社のインフィニオン セキュリティ パートナー ネットワークへの貢献**

インサイトインターナショナル株式会社は、デザインハウスとしてサービスを提供し、顧客が必要とする製品セキュリティに対してソリューション提案やコンサルティング事業も行っています。産業用システムでのIoT端末用に開発したサーバー側で行う管理システムを、顧客にターンキー・ソリューションとして提供し、オープンスタンダードにより製品化までの時間短縮を実現しています。これにより最先端のパートナーとの協働により、多彩なIoT機器を柔軟にシステムに組み込むことができます。

Published by
Infineon Technologies AG
81726 Munich, Germany



Date: 07 / 2017

**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).

**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.

**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.