# “Using TPM with IoT by David Grawrock”
# TCG/JRFによる要約

December 2015

# アジェンダ

- TPM の基本機能の復習
- IoT 環境での必要要件
- それらを満たすもの＝TPM

# TPM の基本機能の復習

- Root of Trust for Reporting (RTR)
  認証(Attestation)のために必須
- Root of Trust for Storage (RTS)
  保護された記憶機構エリア
- Platform adds Root of Trust for Measurement (RTM)
  認証(Attestation)と保護された記憶機構エリアのために必須
- Isolated execution environment
  暗号鍵のハンドリングする環境を隔離させる機能

TRUSTED COMPUTING GROUP®

# IoTでの要件項目
# “End to End security”の担保は?

Questions apply to any device in the ecosystem

## What device are you （どのようなデバイス?)

- デバイスの属性に関する情報も重要

## What is the software stack （どんなソフトウェアが動作?)

- その実行環境は?

## Is there protected storage on the device (保護された記憶機構?)

- 最低でも鍵で管理されている?

## Is there a Trusted Execution Environment (信頼できる実行環境?)

- ソフトウェア攻撃(もしくはハードウェア攻撃からも)に対抗

TRUSTED COMPUTING GROUP®

# TPM機能の実装

- 必要に応じた形状・サイズで提供可能
  - 半導体のチップ
  - 組込みシステムとして
  - ファームウェアでの実装
  - その他
- 要求に応じた機能を提供
  - 応用プラットフォームに応じた機能
    - センサー、ゲートウェイ、ネットワーク、クラウド
  - ユースケースに応じた機能

TRUSTED COMPUTING GROUP®

# Thank you ☺