

# 計測セキュリティ保証スキームの提案



2018.04.17 計測セキュリティフォーラム

電子商取引安全技術研究組合

植村 泰佳

## なぜ、情報セキュリティ保証か？

- 消費者、末端ユーザの脅威に対する漠然とした不安感
- だが、セキュリティは製品コストに転嫁しにくい
- 製造者の「安全スタンプ」志向
- 誰がセキュリティ保証の責任をとるのか？
- 一度セキュリティが破綻すれば、巨額の損害が発生する
- 損害保険方式が普及しない理由
- 第三者評価・認証方式の普及

## 情報セキュリティ保証スキームのあり方

- 情報セキュリティ保証スキームとは、ユーザの調達仕様である「セキュリティ要求仕様」に基づいてメーカーが自己宣言した設計仕様に、メーカーの製品実装がほんとうに合致しているかを、第三者が評価・認証するスキームである。
- 代表的な事例はISO/IEC15408=CCによる公的評価認証であるが、それよりやや簡易な民間保証スキームも含めて、以下に述べるコンセプトによるスキーム構築が世界的に見ても共通の作法となっている。
- ISO/IEC15408による公的な評価認証の例においては、（認証は、製品のセキュリティ自体を保証するものではないので）損害保険的なビジネススキームは全く存在していない。

## 情報セキュリティ保証スキームは、製品のセキュリティを直接保証するわけではない

- 評価認証によって保証するのは・・・
- メーカーが自己宣言したセキュリティ設計仕様に、メーカーの製品実装がほんとうに合致しているか
- 万一当該製品のセキュリティが破られた場合でも、メーカーが自己宣言した仕様通りの製品実装が為されていれば、評価認証側には、補償責任はない
- ただし、社会的によく知られた攻撃手法に対して、上記の設計仕様が脆弱でないかの検証は、評価認証側で行う

# わかりやすい例え話



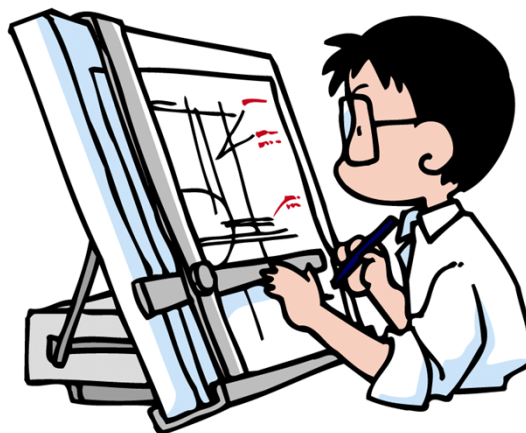
住宅の警備システムを保証しようとする・・・

不動産開発者、住宅メーカー、  
警備会社、警備機器メーカーなどが協議して、  
〇〇地区分譲地用の「セキュリティ要求仕様」をつくる。

PP

セキュリティ要求仕様例：

- ・玄関には電子錠を付けること
- ・すべての窓には警備用センサを付けること
- ・必ずどこかの警備会社と契約すること  
などなど



住宅メーカーは  
「セキュリティ要求仕様」に従って  
住宅を設計する。



住宅メーカーは、住宅購入者にセキュリティ設計仕様を自己宣言する

セキュリティ設計仕様の例:

- ・玄関には〇〇社の△△型電子錠を装備します。
- ・すべての窓に××社のxyz型センサを装備します。
- ・〇〇警備会社と契約し24時間電子警備を実施します…

ST



第三者評価機関が検査すること

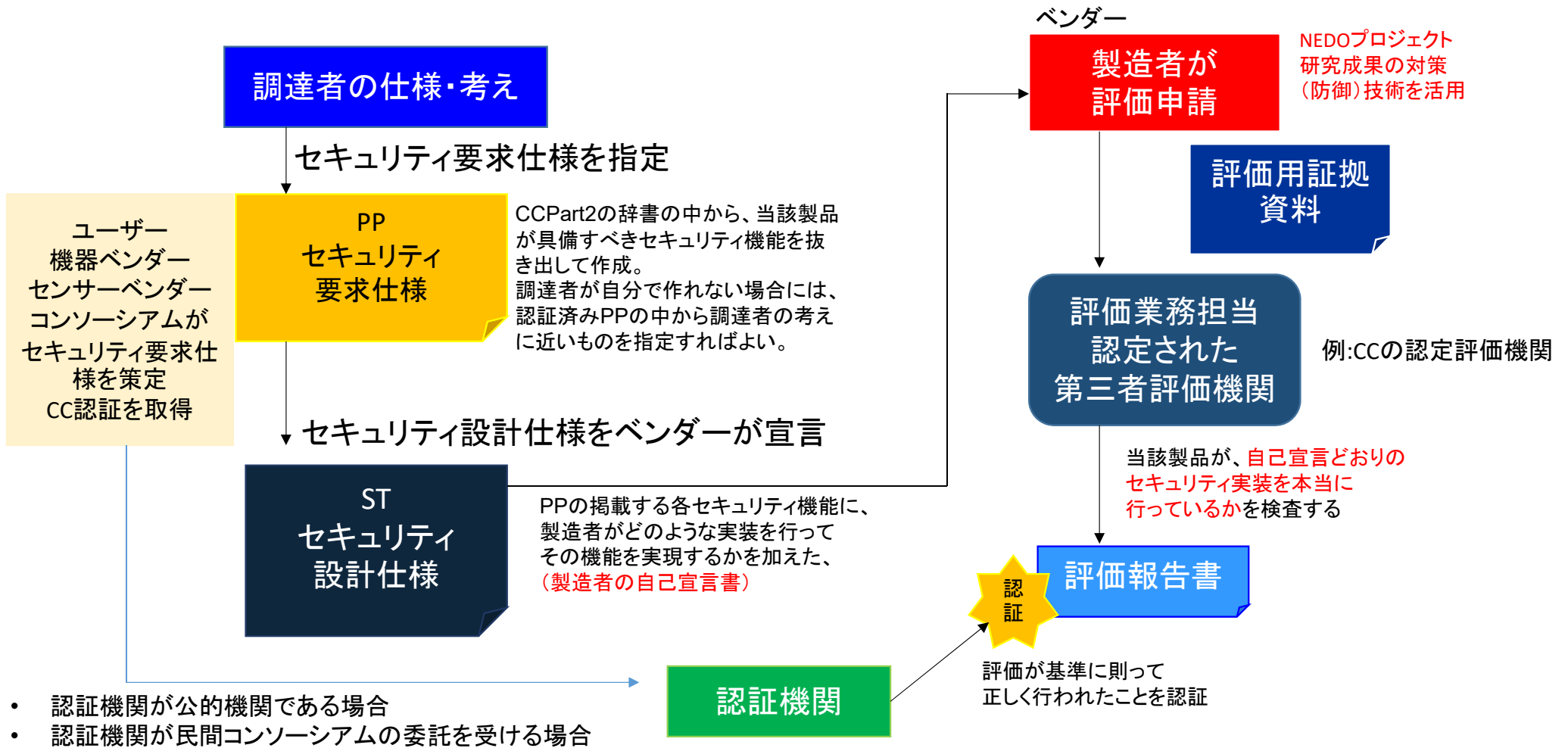
- ・この住宅には、ほんとうにメーカーの宣言した仕様通りの設備が実装されているか
  - ・メーカーの宣言したガイダンスの通り警備は運用されているか
  - ・警備機器は信用のおける会社から納入されているか
  - ・警備機器には脆弱性がないか
- などなど

認証機関が証明すること

この検査は、定められたマニュアル通りちゃんと行われました。



# 情報セキュリティ保証スキームの運用の流れ



計測セキュリティ評価認証スキームの提案 セキュリティ要求仕様と製品評価の対象範囲を下記のとおりとする。  
 ビジネス化が可能な分野から、順次セキュリティ要求仕様の策定と保証スキーム運用を拡大していく。

様々なセンサ	一つのセンサ種類	用途	個別のセンサ
計測セキュリティの対象となるセンサは多種類、多岐にわたっている。 これをまとめて、一つのセキュリティ要求仕様の対象にすることはできない。	例:ライダーセンサ 例:ステレオカメラ用センサ ~ベンダーが特定される	例:自動車運転支援用 例:工場製造列制御用 ~ユーザが特定される	例:〇〇株式会社が製造する製品番号××の自動車運転支援用ライダーセンサ  <div data-bbox="1675 662 2128 880" style="border: 1px solid blue; border-radius: 15px; padding: 10px; text-align: center;">                         評価認証スキーム                          運用開始後の                          製品評価の対象                     </div>

種類と用途を特定した  
 セキュリティ要求仕様  
 (ユーザがベンダに要求する)

例:自動走行支援用  
 ライダーセンサの  
 セキュリティ要求仕様

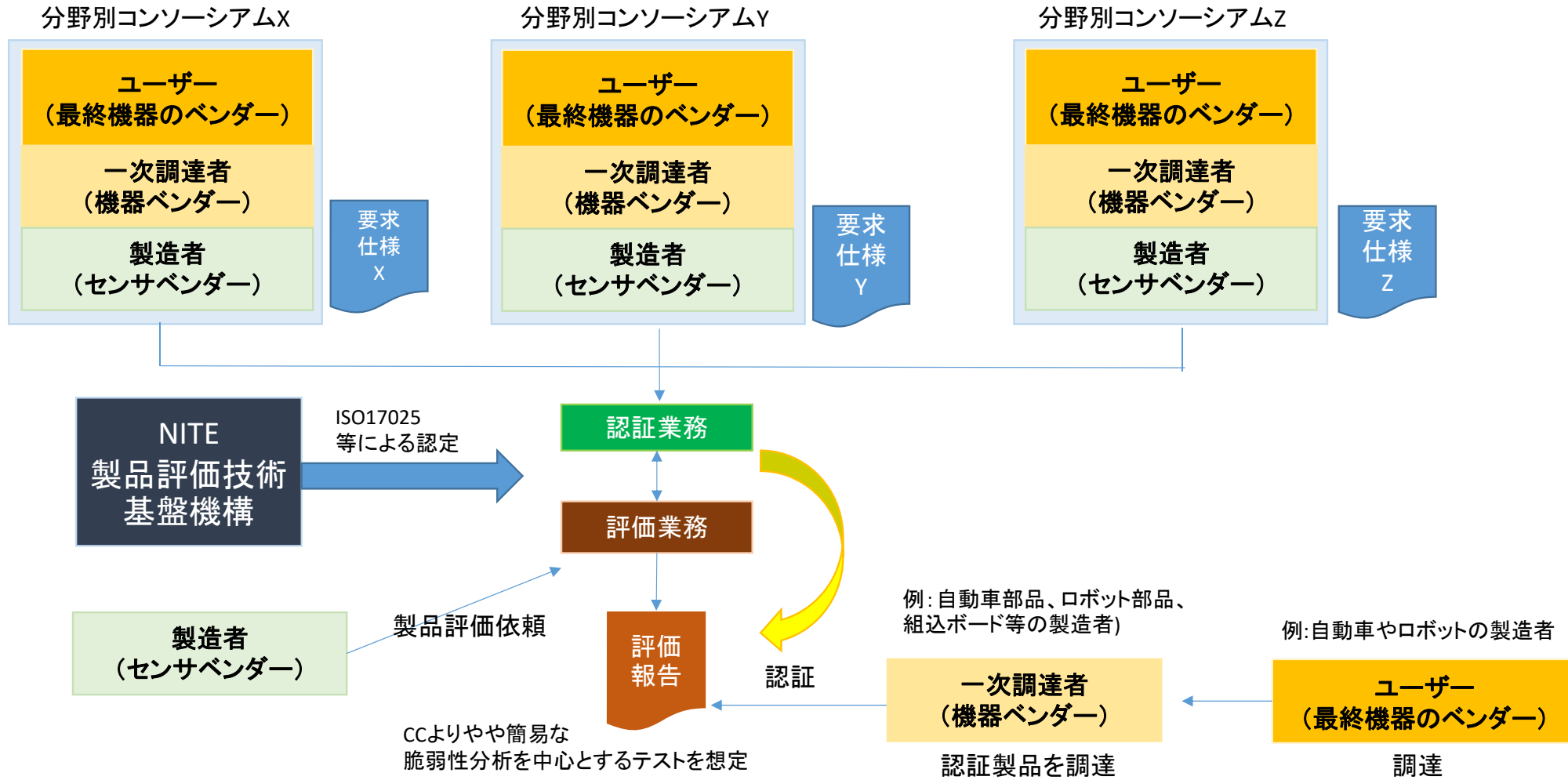
当該製品が、  
 セキュリティ要求仕様に  
 合致しているかを  
 評価する。

コンソーシアムごとに  
 複数のセンサ製品分野の  
 セキュリティ要求仕様を策定し  
 運用する。

例の場合:ユーザ(最終ユーザ及び/又は自動車部品の一次メーカー)と  
 ライダーセンサのベンダによるコンソーシアムが保証スキームを運用

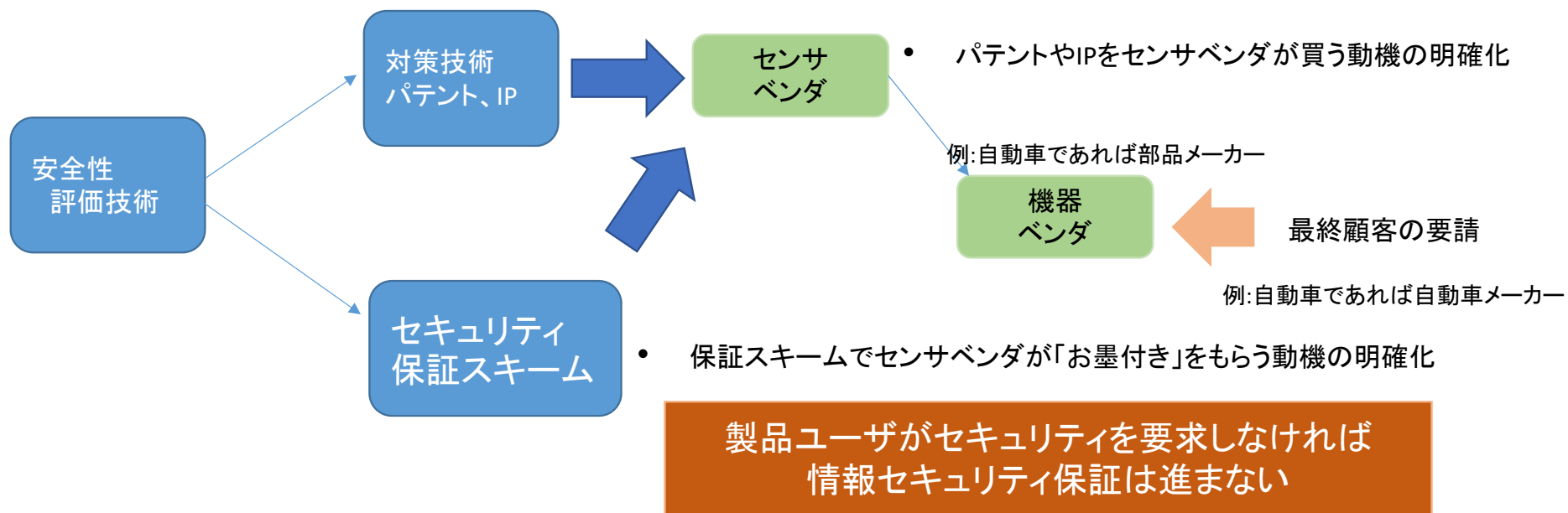


# 現在想定する計測セキュリティ保証スキームの概要



## 計測セキュリティ保証スキーム構築に向けた課題

- パテントやIPをセンサベンダが買う動機の明確化
- 保証スキームでセンサベンダがお墨付きをもらう動機の明確化
- 全く新しい分野、概念のセキュリティ技術であるため、ベンダー、ユーザーへの啓蒙から始めなければならない。本事業対象分野のセンサベンダーには、Safetyの意識は若干あったが、センサが計測するデータそのものが改ざん、変改されるというSecurityに対する意識がまだ普及していない。
- 計測セキュリティの概念が普及するにつれて、国際間のセキュリティ技術開発競争、標準化競争が激化する。



## ポイント

- 情報セキュリティをIoTの様々な分野で普及させるためには、ユーザ、機器ベンダー、部品ベンダー、テスト機関、認証機関などの各レイヤーのプレイヤーが、情報セキュリティに関する認識を共有することが必要
- セキュリティビジネスは上記の認識共有がなければ成立しない
- 「セキュリティ要求仕様」策定のためのコンソーシアム活動が、認識共有のための契機となる

謝辞:

このプレゼンテーションに示す成果の一部は、  
国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)の  
委託業務の結果得られたものである。



お問い合わせ先: [uemura@ecsec.org](mailto:uemura@ecsec.org)