第1回　STAMPワークショップ in Japan

UNISYS

UCA抽出における Extending STPAの試行 ～農園ビジネスへの適用～

2016年12月 7日

日本ユニシス株式会社
総合技術研究所
福島　祐子

Foresight in sight

1 STAMP/STPA適用の動機

2 STAMP/STPAを進める上での課題

3 Extending STPA の概要

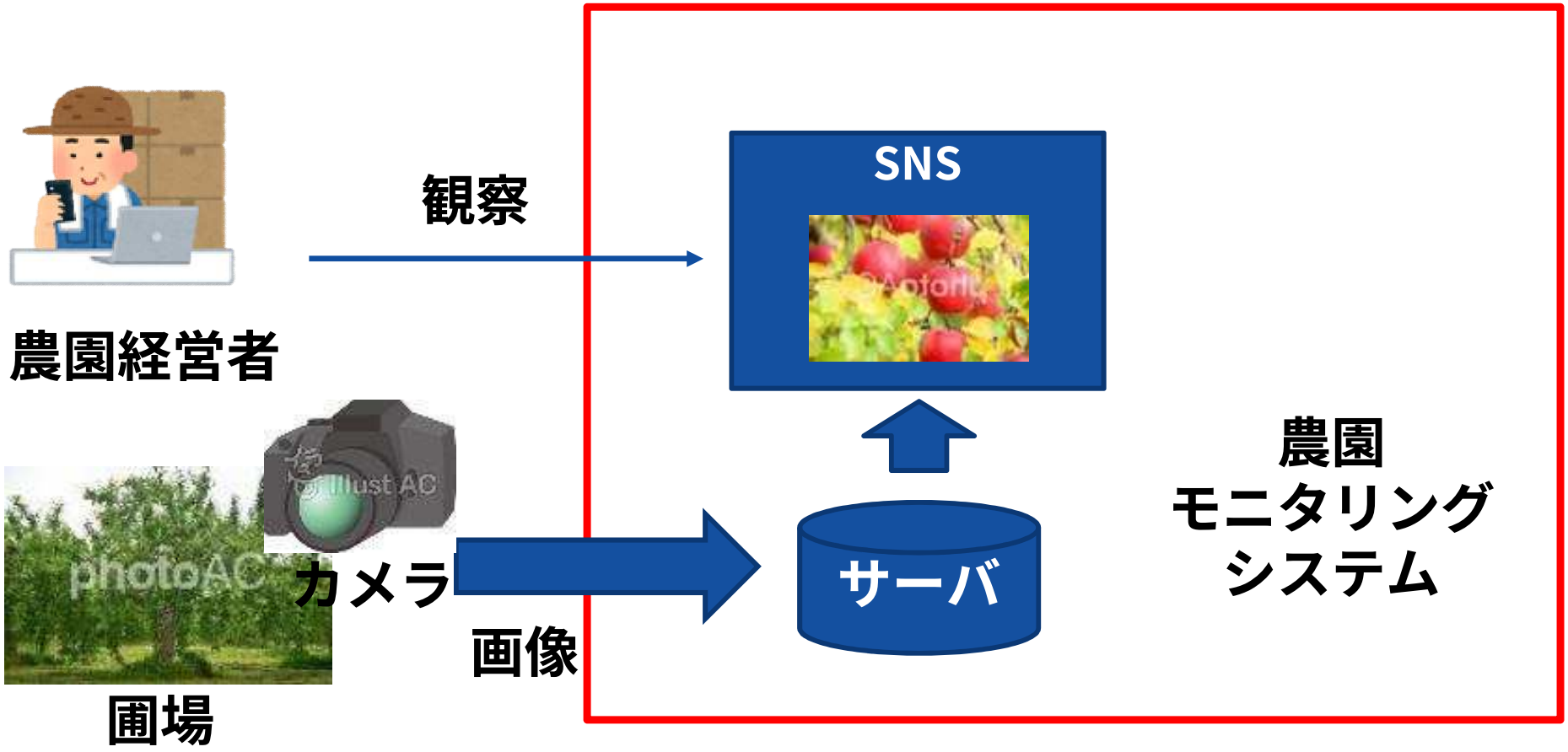
4 Extending STPA の試行 ー 農園ビジネス

5 まとめ

STAMP／STPA適用の動機

- 農園モニタリングシステム（信州大学・大阪大学との共同研究）

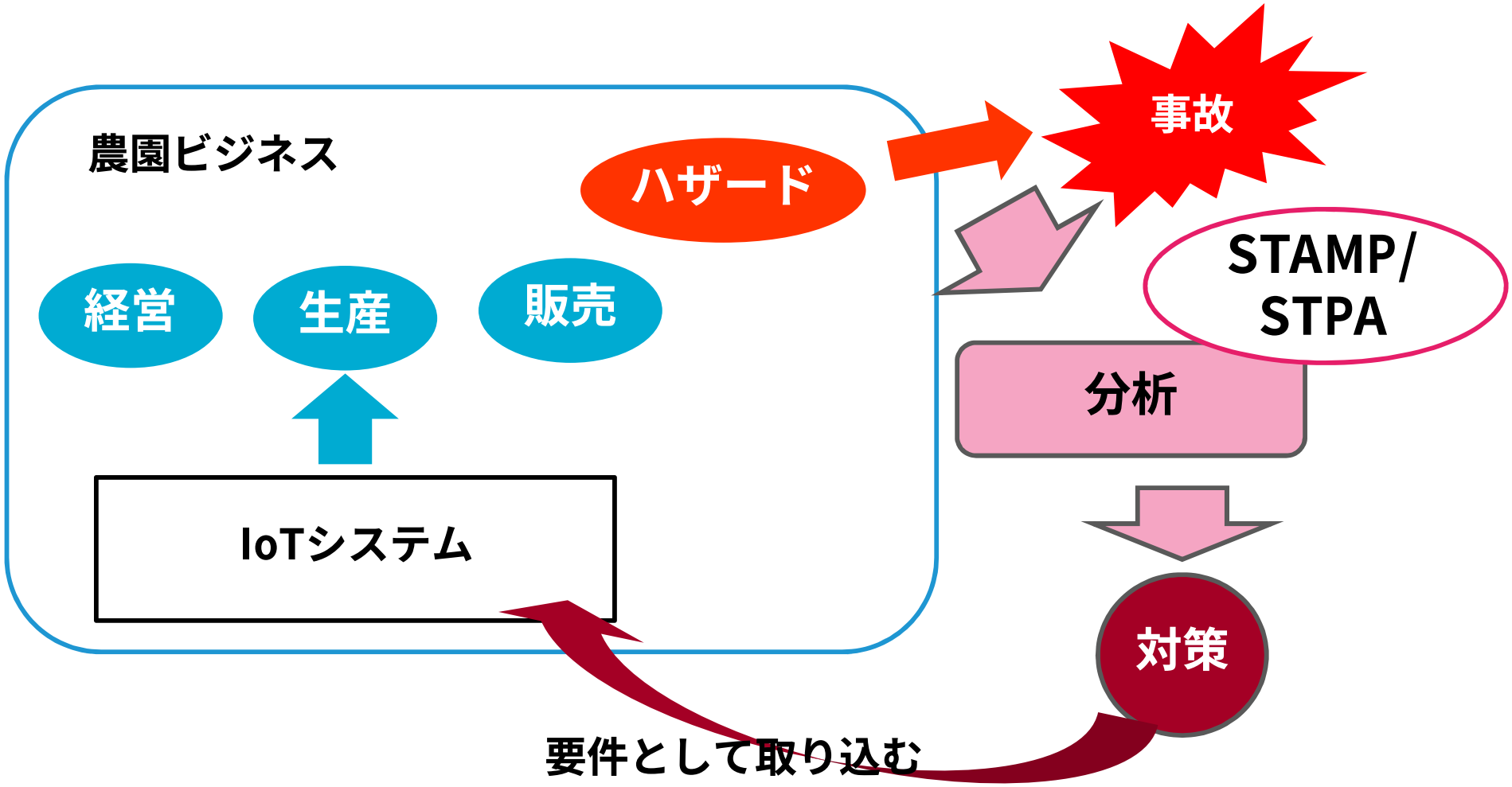
農園経営者による農作物の生育状況の観察を容易にする



STAMP／STPA適用の動機

農園ビジネスの安全性について考えたい

- 農園ビジネスそのものの安全性を解析
- 安全性への対策を「IoTシステム」で実現



STAMP/STPAを進める上での課題

① 事故、ハザード、安全制約における考え方

事故やハザードは誰が識別するのか、高レベルなハザードをどのように識別するのか？

② コントロールストラクチャ構築における考え方

抽出するコンポーネントの粒度、範囲をどうするか？

③ プロセスモデル特定の方法

1. プロセスモデルはどのタイミングで特定するのか？
2. プロセスモデルはどのように考えて特定するのか？

■ ①、②、③-1は、“Engineering a Safer World”により解決。（「付録１」参照）

■ 「③-2　プロセスモデルはどのように考えて特定するのか」は未解決。

→ Extending STPA　（MIT John Thomas氏提唱）を発見！

Extending STPAの概要

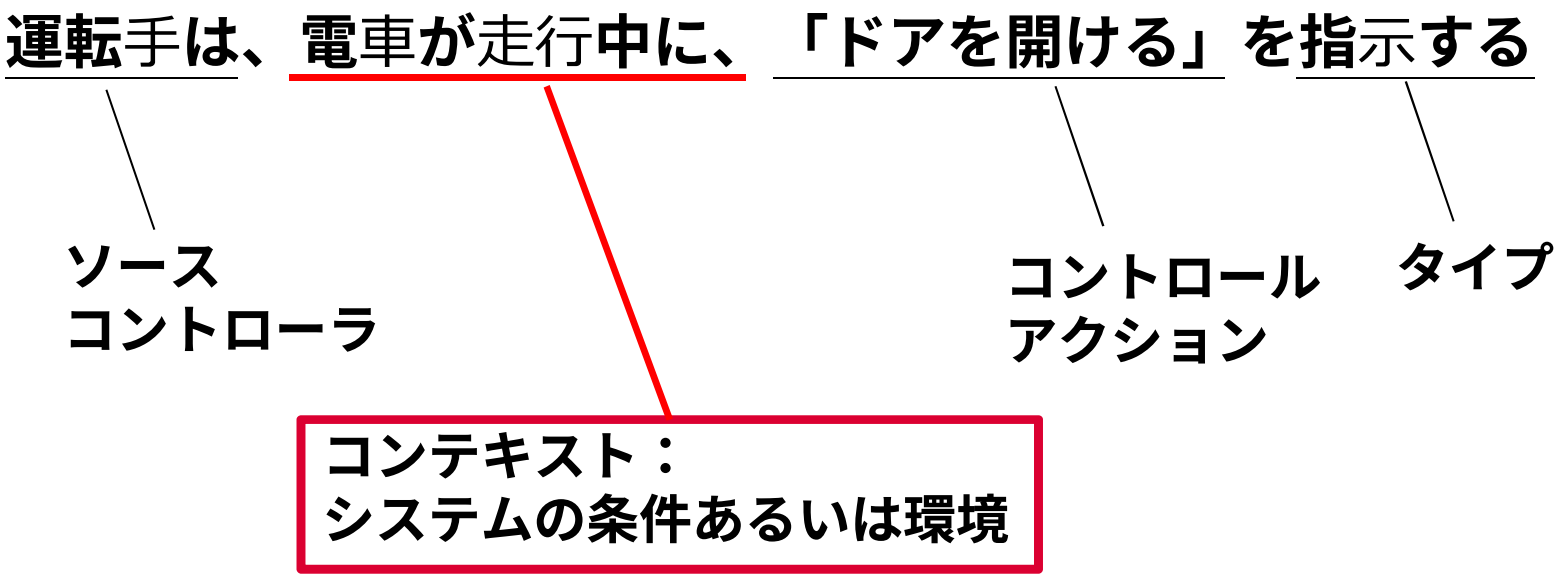
- 現在のSTPAの問題点
  - ハザードにつながるコントロールアクションの識別はアドホックである。ハザードコントロールアクションを表す４種類のガイドワードが示されているだけである。

Extending STPA：
ハザードにつながるコントロールアクションの識別を支援

Extending STPAの概要 ー 考え方

- 「ハザードにつながるコントロールアクション」の**構造を定義**
- **コンテキストの情報**が重要（ハザードにつながるか決まる）

ハザードにつながるコントロールアクションの構造例：

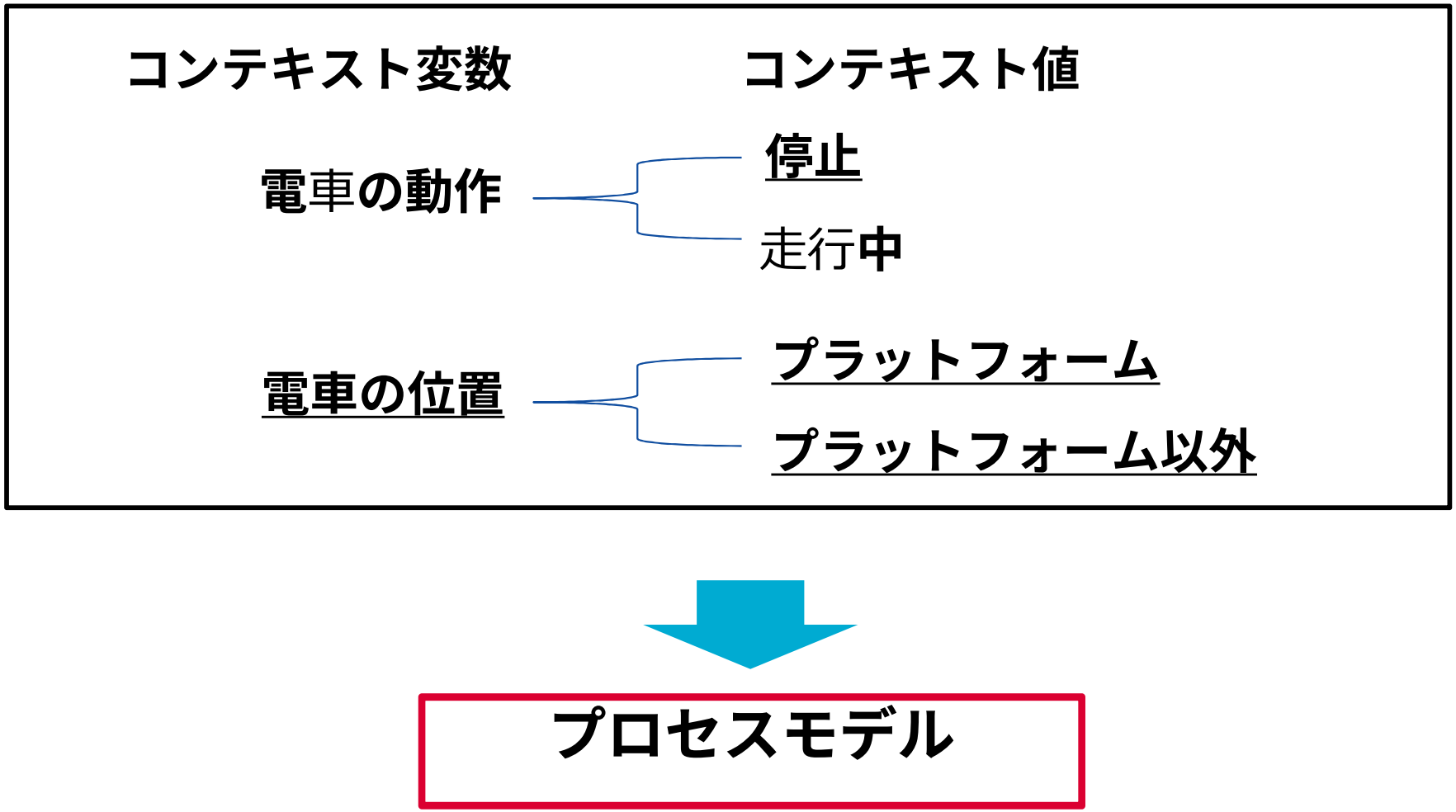


コントローラは、コンテキストを把握する必要がある！

Extending STPAの概要 ー 考え方

- コンテキストを分解して、追加のガイダンスを得る

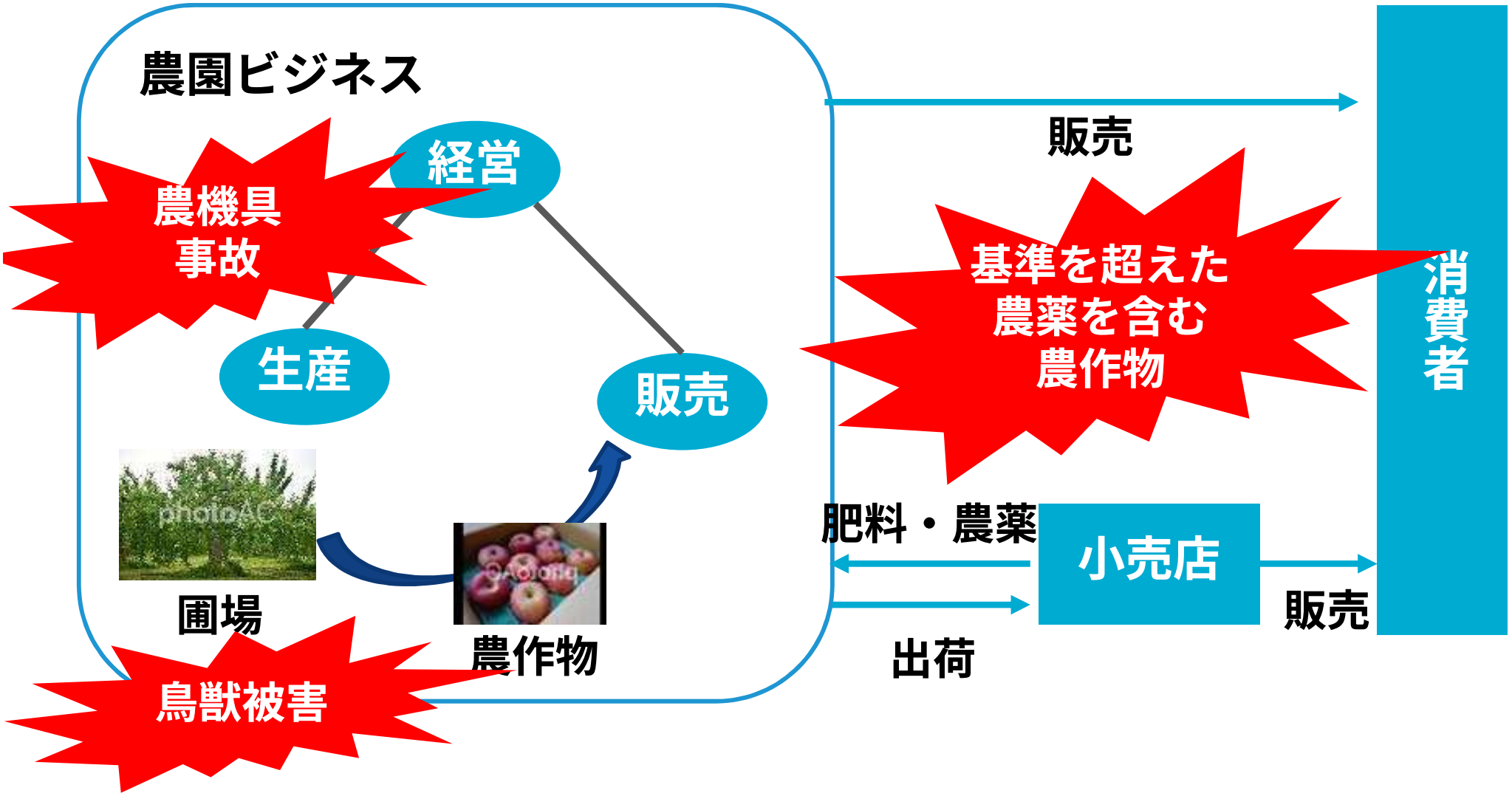
コンテキスト「電車の走行中」の分解例：



Extending STPA試行 ー 農園ビジネス

Foresight in sight

■ 農園ビジネスにおける事故とは



Extending STPA試行 ー 農園ビジネス

Step0準備１：事故、ハザード、安全制約の識別

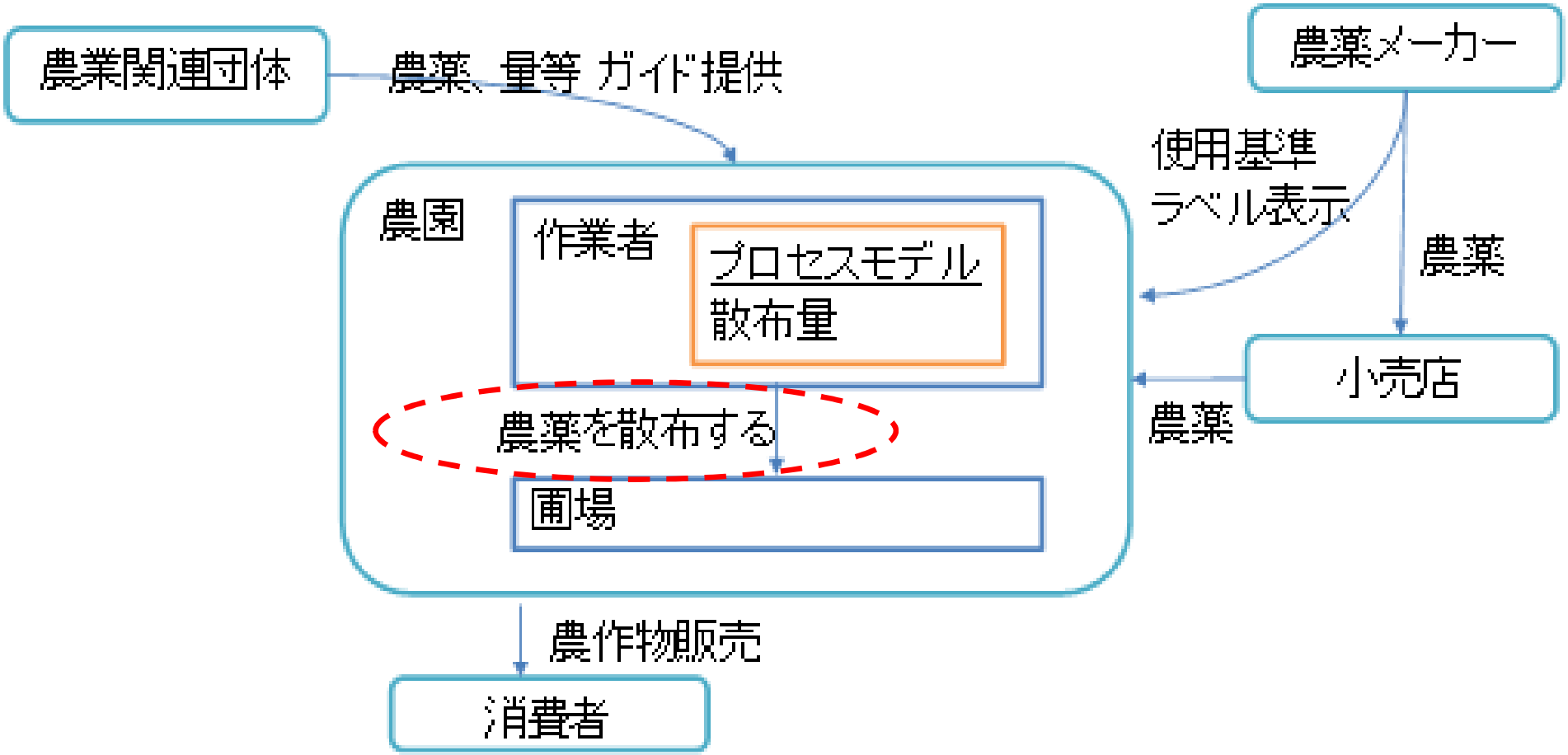
事故：基準値以上の残留農薬を含む農作物が市場に出回る

ハザード：
基準値以上の残留農薬を含む農作物を出荷する

安全制約：
基準値以上の残留農薬を含む農作物を出荷してはならない

Step0準備２：コントロールストラクチャの構築

ハザード：基準値以上の残留農薬を含む作物の出荷



Extending STPA試行 ー 農園ビジネス

UCA（安全ではない Control Action）の識別（従来手法）

コントロールアクション	「Not Providing」 が ハザードを引起す	「Providing」 が ハザードを引起す	「Wrong Timing / Order」 が ハザードを引起す	「Stopping Too Soon/Applying Too Long」 が ハザードを引起す
農薬を散布する	ー	（UCA1） 規定値以上の農薬を散布する	（UCA2） 農薬の散布が遅すぎる	ー

UCA１：規定値以上の農薬を散布する

HCF(ハザード原因要因)：散布量が規定値以上であるのに、作業者が規定値未満と認識している

Extending STPAを適用

ハザードにつながるコントロールアクション：

作業者が、散布量が規定値以上なのに、農薬を散布する

コンテキスト変数	コンテキスト値
散布量	規定値以上　or　規定値未満

初期のプロセスモデル

Extending STPAを適用

初期のプロセスモデル：

プロセスモデル変数	規定値以上の散布量
	規定値未満の散布量

分解

「散布量が規定値以上」というのは
どういうことか？
いつ　どこに　何を

プロセスモデル階層：

規定値以上の散布量
- 今回の散布量　　規定値以上　規定値未満
- 過去の散布量　　規定値以上　規定値未満
- 散布エリア
  - 今回の散布エリア　　正しいエリア　誤ったエリア
  - 過去の散布エリア　　正しいエリア　誤ったエリア

Extending STPA試行 ー 農園ビジネス

■ 詳細化したプロセスモデルからUCAを特定

従来手法：

（UCA1）規定値以上の農薬を散布する

Extending STPA：

（UCA1-1）今回の散布量が規定値以上であるが、農薬を散布する

（UCA1-2）過去の散布量が規定値以上であるが、農薬を散布する

（UCA1-3）今回の散布エリアが誤っているのに、農薬を散布する

（UCA1-4）過去に対象エリアに誤って農薬を散布しているのに、重複して農薬を散布する

Extending STPA試行 ー 農園ビジネス

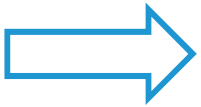
■ ハザードにつながる一つのシナリオ

作業者１が、エリアAに農薬を散布するところを誤ってエリアBに散布する。（エリアを誤認識する）
作業者２が、正しい散布エリアとしてエリアBへ農薬を散布する。（エリアBへの誤った散布を知らない）
これにより、エリアBに規定値以上に農薬が散布される。

■ 対策

誤ったエリアであることを作業者が認識できるようにする

GPSにより作業者の位置を特定。
散布器具にセンサーを取り付け、誤った散布エリアで散布するとアラームが鳴る。



「IoTシステム」の要件へ

まとめ

- 今回の試行でできたこと
  - 顧客ビジネスの安全性解析にExtending STPAを適用することで、システム要件に取り込むことができる具体的な対策を得た。

- 今回の試行で確認できたこと
  - プロセスモデルの重要性
    - プロセスモデルはコントローラのUCA実行の判断材料なので重要である。
    - UCA、HCFの具体性は、プロセスモデルの明確さに依存する。
  - Extending STPAの有効性
    - Extending STPAの考え方は、プロセスモデルを明確にするのに有効である。

付録１ STAMP/STPA適用のコツ（抜粋）

- 事故の識別
  - 何を事故とするのかという定義は安全性への取り組みのゴールとスコープになるので、取り組みを開始する前に定義しなければならない。
  - 事故は、顧客、システムの統制機関、ユーザグループ、保険会社、専門団体体、業界標準、その他の利害関係者などから引き出す。

    ・・・
- ハザードの識別
  - ハザード識別の前にシステム境界を決める。境界を定義するよい方法は、アクシデントに関係する条件のうちデザイナがコントロールできる条件を含めるようにすることである。
  - ハザードには、“故障（failure）”、“エラー（error）”という用語がふくまれている場合には、誤っている可能性がある。“故障”、“エラー”はハザードそのものではなく、ハザードにつながる原因であることが多い。ハザードとその原因を分けることが重要である。

    ・・・

（Nancy Leveson, *Engineering a Safer World*, The MIT Press, 2012）

参考文献

- **はじめての**STAMP/STPA ～**システム思考に基づく新しい安全性解析**手**法**～, IPA/SEC, 2016, http://www.ipa.go.jp/files/000051829.pdf
- Nancy Leveson, An STPA Primer, http://psas.scripts.mit.edu/home/wp-content/uploads/2015/06/STPA-Primer-v1.pdf
- Nancy Leveson, Engineering a Safer World, The MIT Press, 2012
- John Thomas, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, http://sunnyday.mit.edu/JThomas-Thesis.pdf
- 小**林一樹**, **作物の生育情報抽出のための高精細画像比較システムの開発**, https://www.jstage.jst.go.jp/article/air/22/1/22_24/_pdf, 2013

Foresight in sight

UNISYS

ご清聴ありがとうございました