STAMP/STPA
～業務系システムへの応用検討～
A Study of Applying STAMP/STPA to an Enterprise System

1st STAMP Workshop in Japan
2016年12月6日

IPA/SEC「システム安全性・信頼性分析手法WG」委員
日本電気株式会社　向山　輝

IPA/SEC「システム安全性・信頼性分析手法WG」

- 2015年4月：設置
- 2015年度：主な活動
  - 単線鉄道の踏切制御システムを対象としたSTPA分析事例創出
  - 初心者向けの解説書「はじめてのSTAMP/STPA」を発行
  - 13th WOCS2（2016/1）Nancy Leveson教授、Dr. John Thomas氏を招聘し意見交換会を開催
- 2016年度：主な活動
  - JASPARとの活動連携を開始
  - 人・組織間の指揮系統の分析への拡張（踏切管理システム更新工事）
  - エンタープライズ系（業務系）への応用検討

    ・・・など

本発表では、当WGで調査を進めている
「エンタープライズ系への応用検討」について紹介

- WGで検討中の内容と、これまでに得られた結果を報告します。

背景・動機 Background and Motivation

SEC Software Reliability Enhancement Center

背景 Background

- STAMP/STPAの利用事例は、自動車、航空機、鉄道などの機器を制御するシステムの事例が多い。しかし、業務系でもシステム障害が社会的・経済的に大きな損失につながる「事故」が増えている
  Enterprise systems can also involve unacceptable losses.
  - 例）銀行勘定系、交通機関旅客システム、携帯電話インターネット接続サービスなど
- ICT技術の進歩にともない、システム同士が連携するサービスが拡大
  ⇒ 大規模・複雑化により、起こり得る事象の把握が困難に

動機（確認したいこと）Motivation (What we want to make sure)

- 業務系システムに対してSTPA分析の手法は適用可能か？
  How is STPA applicable to enterprise systems?
- 業務系システムに対してSTPA分析を行う場合、（制御系の場合と異なる）特有の作業や注意点が必要か？
  Any features specific to applying STPA to enterprise systems?

業務系システムにSTPA分析を適用する試行を実施

SEC Software Reliability Enhancement Center

例題：通販業務システム
Targeted example: (fictional) Mail-order shopping system

- 多くの人が利用者として関わった経験があり、業務内容を想像しやすい

行った作業 What were done for the trial

(1) 試行の例題とする業務システムの仕様の決定

Define spec. of the mail-order shopping system

※ 架空の業務システムを例題としたため、仕様を定義する作業が必要であった。

(2) 分析対象とする事故の定義、ハザード、安全制約の識別

Identifying accidents, hazards and safety constraints

(3) 制御構造モデルの構築

Constructing control structure

(4) UCA（Unsafe Control Action）の識別

Identifying UCAs

(5) UCAの原因の識別

Identifying the causes of the UCAs

(1) 例題とする業務仕様の決定
Specification of the mail-order shopping business (system)

SEC Software Reliability Enhancement Center

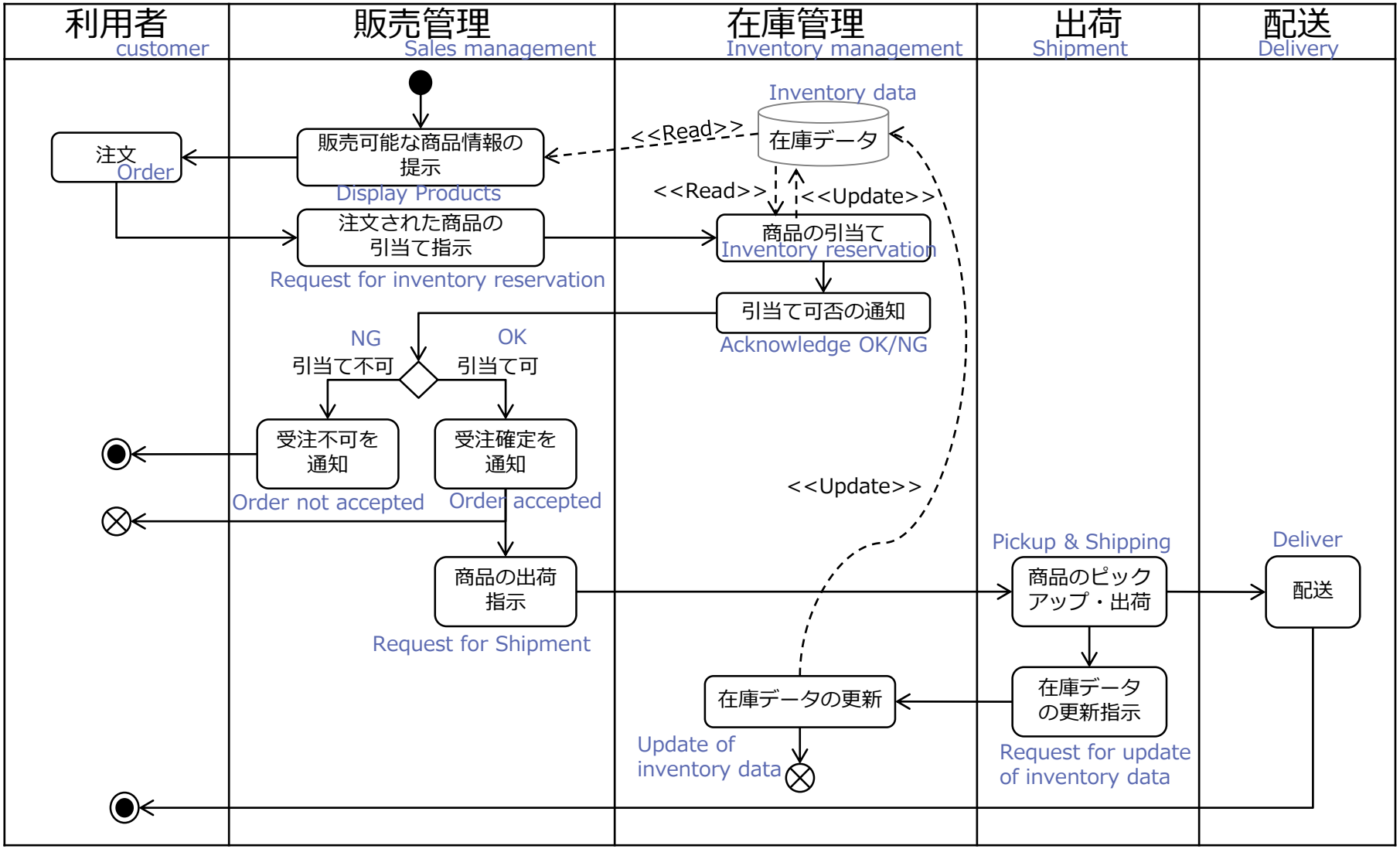
- 業務の目的 Purpose of the business
  - 利用者からの注文を受け、注文された商品を配達する。
    Deliver the ordered products to the customer.

- 業務の内容 Details of the business

機能 Functions	業務内容 Details
販売管理 Sales management	– 販売可能な（在庫のある）商品の情報を利用者に提示する。 – 利用者からの注文を受けると、商品の引当てを行い、受注確定を利用者に通知する。引当てができない場合は、受注不可を利用者に通知する。
在庫管理 Inventory management	– 注文された商品の引当てを行い、重複受注を防ぐ。 – 商品の出庫・入庫に応じて在庫数を更新し、在庫の問合せに対応する
出荷 Shipment	– 注文された商品をピックアップし、出荷する。
配送 Delivery	– 出荷された商品を目的地まで配送する。

業務系システムで一般的に使われるアクティビティ図
（業務フロー図）で表現
Expressed by UML Activity Diagram

アクティビティ図による業務仕様の表現
Business specification expressed by Activity Diagram



STPA分析の試行上の前提
Assumptions made for the trial

SEC Software Reliability Enhancement Center

■ システム化範囲に関する前提

- 販売管理と在庫管理はシステム化され、自動処理されるとする
- 出荷と配送は人手作業で行われるとする
- Sales management and Inventory management are automated.
- Shipping and Delivery are manual work.

■ 配送に関する前提

- 出荷された商品は、確実に顧客のもとに配達されるものとする
- Delivery is carried out properly (with no delay, no mistakes)

(2) 事故の定義、ハザード・安全要件の識別

SEC
Software Reliability Enhancement Center

事故 Accident	ハザード Hazard	安全制約 Safety Requirement
注文した商品が、顧客に配達されない Ordered product is not delivered to the customer	受注確定後、注文された商品が出荷されない状態 After order is accepted, the ordered product is not shipped	受注が確定したら、速やかに、商品が出荷されなければならない Once order is accepted, the ordered product should be promptly shipped

(3) 制御構造モデルの構築
Creating Control Structure Diagram

SEC Software Reliability Enhancement Center

- 業務仕様から如何に制御構造モデルを構築するか
  - 慣れた人が暗黙的に行う手順を明文化したい

- アクティビティ図を参照した手順を考案
  Procedure for drawing control structure utilizing Activity Diagram

①アクティビティ図から、安全制約に関係する「処理」と「機能」を抽出
Identify actions and functions related to “safety constraints” in the activity diagram

↓

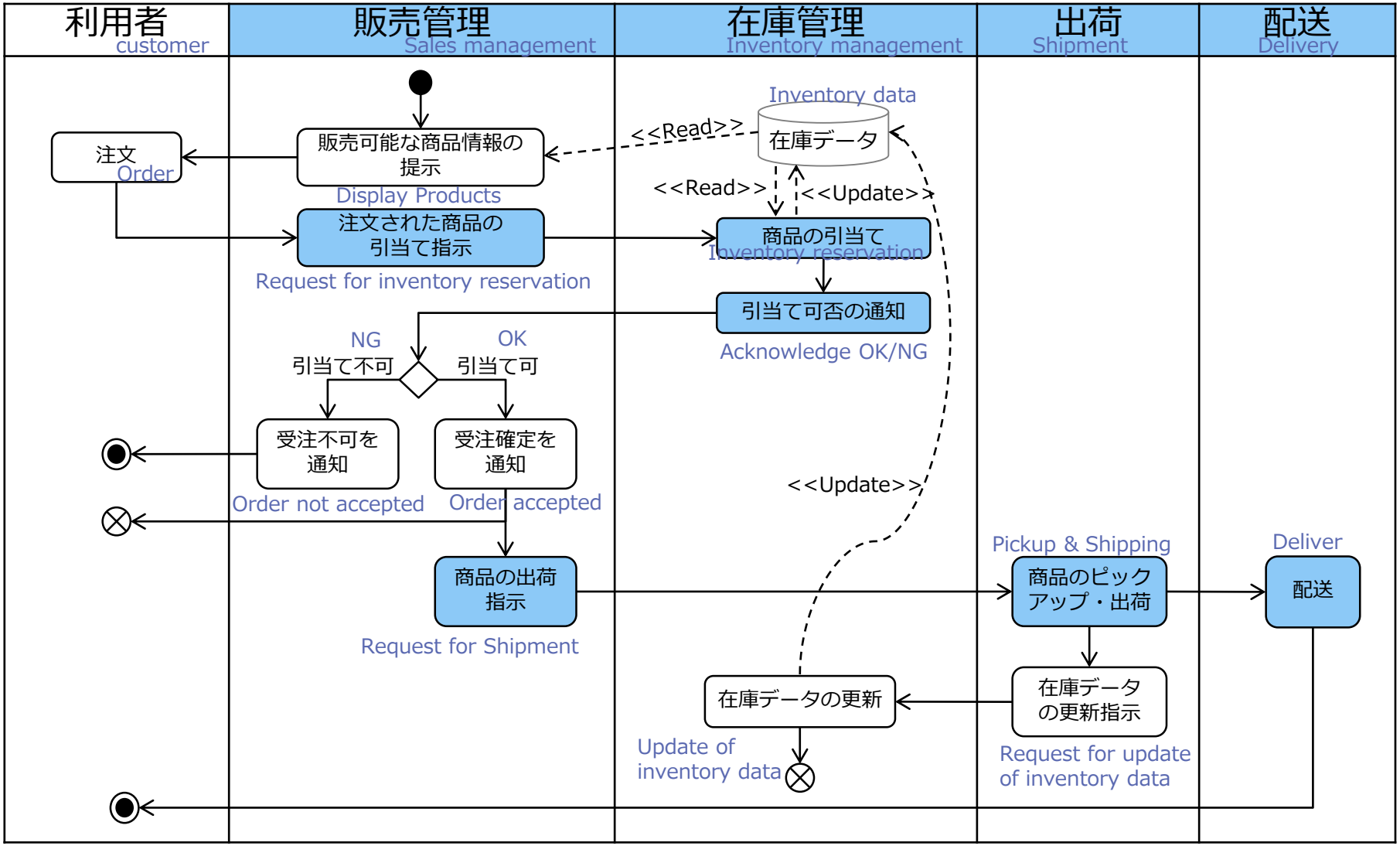
② 抽出した結果から、以下の方針で制御構造モデルを作成
Create control structure diagram according to the following policy

- 「機能」をコンポーネントとする
  Consider functions as “components”
- 機能間をまたぐ「処理」をコントロールアクションの発行、またはフィードバックデータの発行と考える
  Consider the action that acts across functions as either “control action” or “feedback”

(3) 制御構造モデルの構築　－①

SEC Software Reliability Enhancement Center

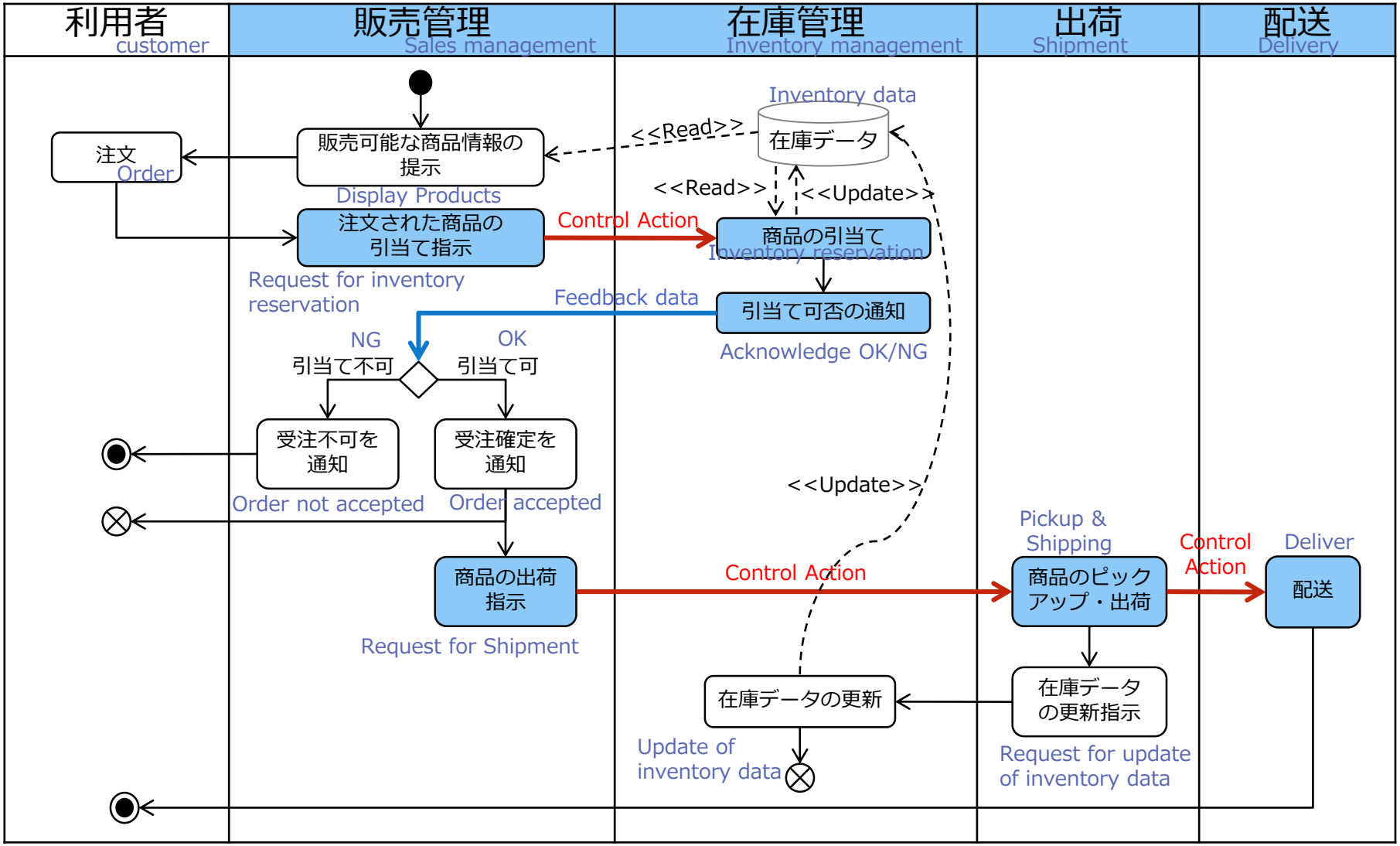
■ 安全制約に関わる「処理」と「機能」を抽出（水色で表示）



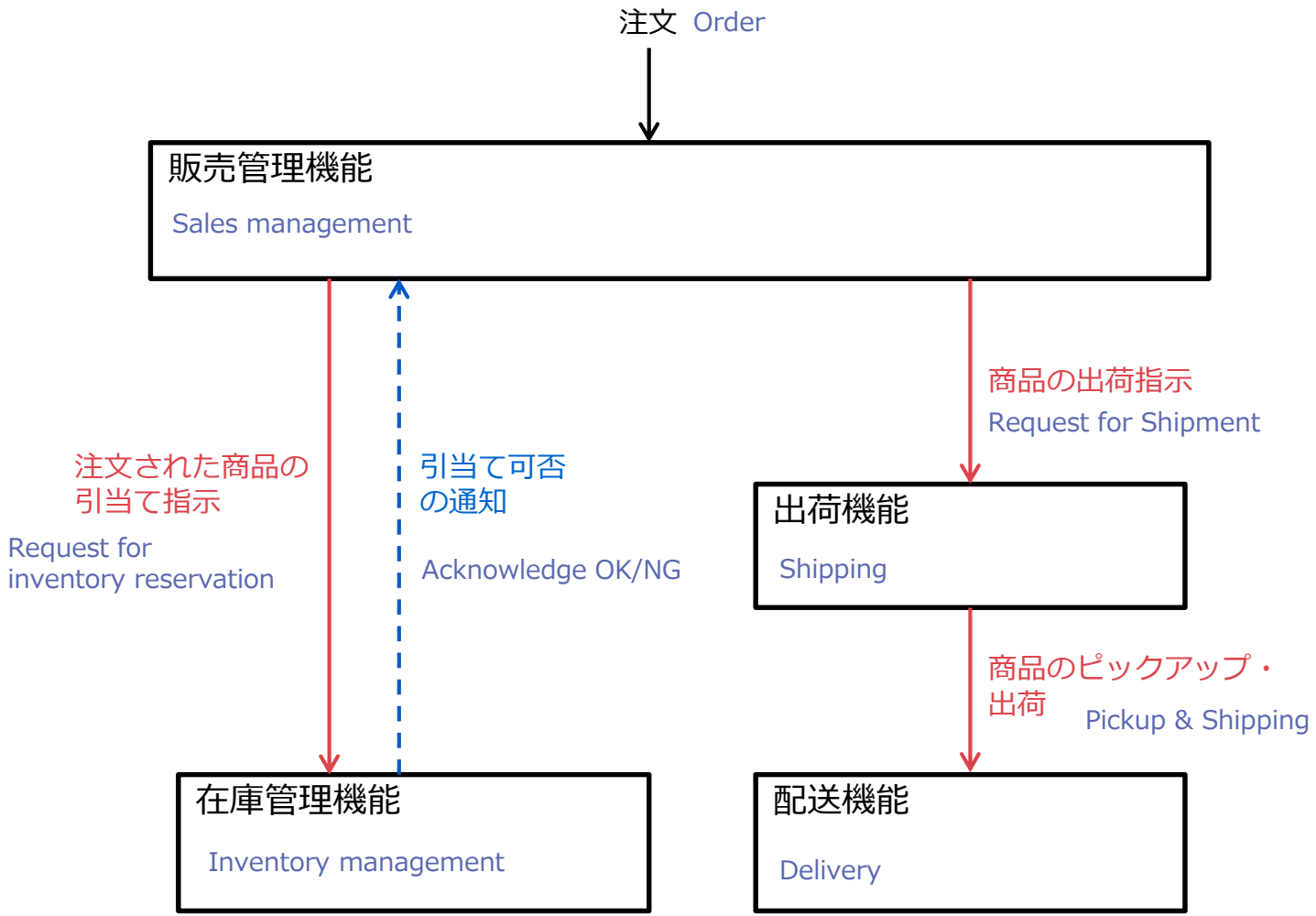
(3) 制御構造モデルの構築　－②

SEC Software Reliability Enhancement Center

■ 機能をまたぐ「処理」をCAまたはFBとする



(3) 制御構造モデルの構築
Control Structure Diagram



(4) UCAの識別
Identifying UCAs

SEC Software Reliability Enhancement Center

コントローラ ↓ 被コントローラ	制御アクション	ガイドワード			
		Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order causes hazard	Stopping too soon/applying too long causes hazard
販売管理機能 ↓ 在庫管理機能	商品の引当て指示	**(UCA1)**注文された商品の引当てが行われず、重複受注が発生する。その結果、出荷時に商品が不足し、出荷できない。	注文されていない状況で引当て指示が発行される。その結果、引当て可能在庫数が実際より少なくなり、販売機会を失う。 →安全制約違反ではない。	注文される前に引当て指示が発行される。その結果、引当て可能在庫数が実際より少なくなり、販売機会を失う。 →安全制約違反ではない。	–
販売管理機能 ↓ 出荷機能	出荷指示	**(UCA2)**受注が確定したにもかかわらず、出荷指示が発行されない。	**(UCA3)**在庫が無い状況で出荷指示が発行される。	**(UCA4)**引当て可否が通知される前に出荷指示が発行される。	–
出荷機能 ↓ 配送機能	ピックアップ・出荷	**(UCA5)**出荷指示が発行されたが、ピックアップ・出荷が行われない。	**(UCA6)**出荷指示と異なる商品がピックアップ・出荷される。	出荷指示を受けた後、ピックアップ・出荷が遅すぎる。 →UCA5と同じ。	–

(5) UCAの原因の識別
Identifying the causes of the UCAs

- **UCA１：「注文された商品の引当てが行われない」**
  Request for inventory reservation is not provided for ordered product.
- **UCA２：「受注が確定したにもかかわらず、出荷指示が発行されない」**
  Order is accepted, but request for shipment is not provided.
- **UCA４：「引当て可否が通知される前に出荷指示が発行される」**
  Request for shipment is provided before receiving result of inventory reservation.

⇒ **発生原因：**

販売管理と在庫管理はシステム化され、自動処理されるため、
これらのUCAの発生原因は考えにくい

※ プログラムのバグがあれば上記UCAの発生は考えられるが、
今回のSTPAの試行では扱わない

By the assumption that sales management and inventory management are automated, these UCAs unlikely occur.
Program bugs could be causes for these UCAs,
but in this trial, we don’t analyze such causes for the UCAs.

(5) UCAの原因の識別
Identifying the causes of the UCAs

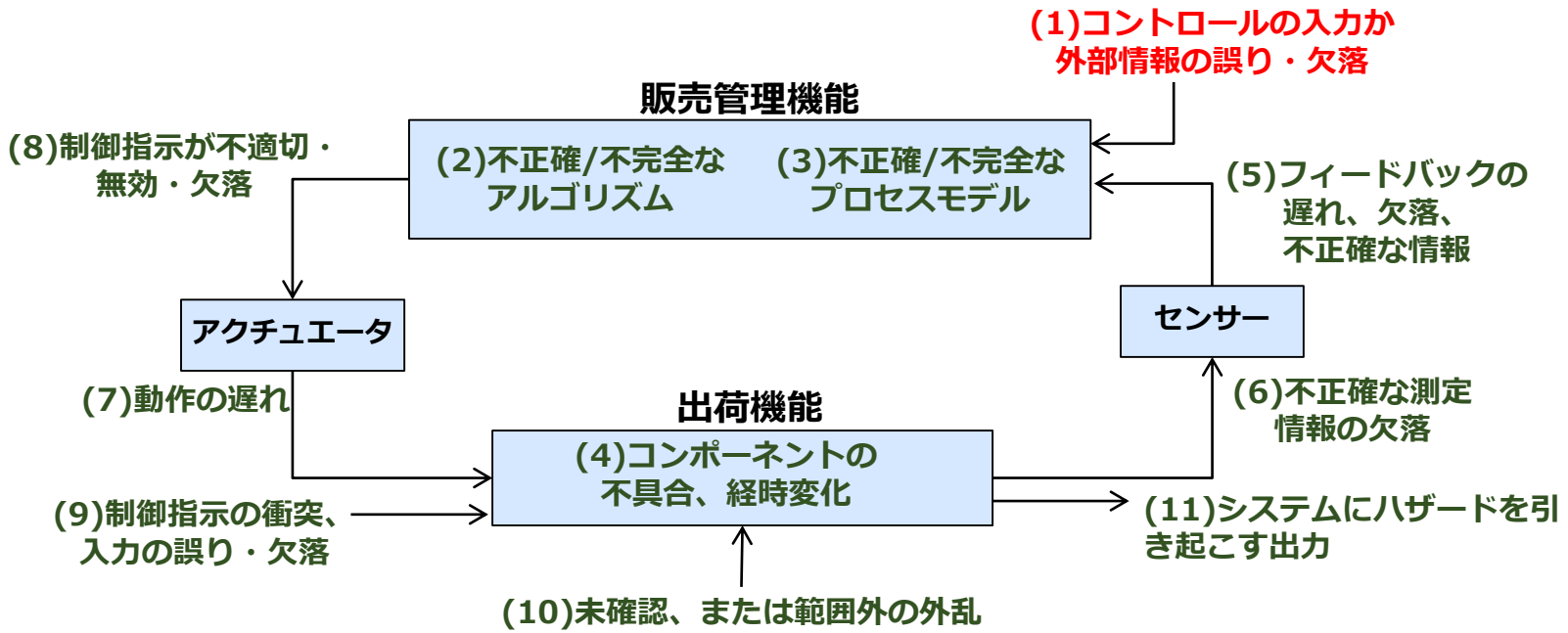
- **UCA３：「在庫が無い状況で出荷指示が発行される」**
  Request for shipment is provided when there is no enough stock.

⇒ 考えられる原因： Cause of the UCA

在庫が無いにもかかわらず、「引当て可」が通知され、出荷指示が発行される。
その原因として、在庫データ更新の遅延/欠落による実態との乖離が考えられる。
"Inventory reservation is OK" is acknowledged when actual stock is not enough.

⇒ 導かれる安全要件： Safety Requirement

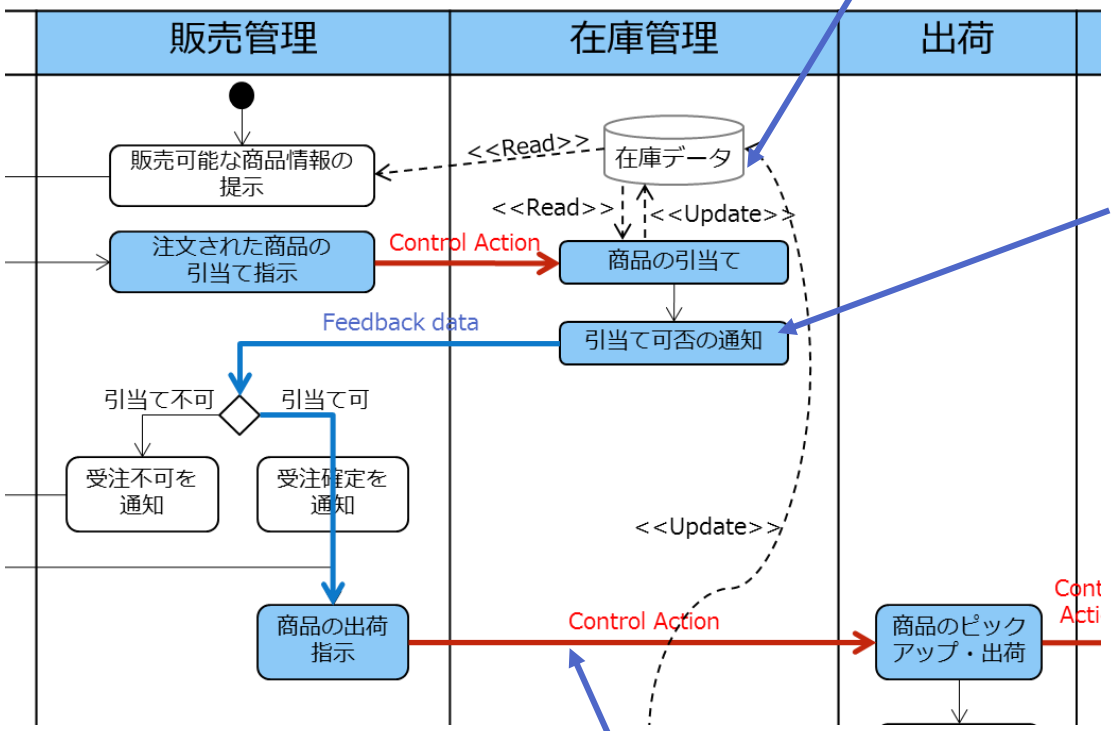
商品の引当てを行う前に、在庫データの更新が完了していること。
Update of inventory data must be completed before providing inventory reservation.



(5) UCAの原因の識別
Identifying the causes of the UCAs

原因：在庫データの更新が欠落または遅延し、在庫数が不正となる。

data is incorrect due to lack or delay of updating data.



そのため、在庫が無いにも関わらず「引当て可」が通知される。

due to incorrect data, “OK” is feedback despite there is no enough stock.

UCA３：「在庫が無い状況で出荷指示が発行される」

Request for shipment is provided when there is no enough stock.

(5) UCAの原因の識別
Identifying the causes of the UCAs

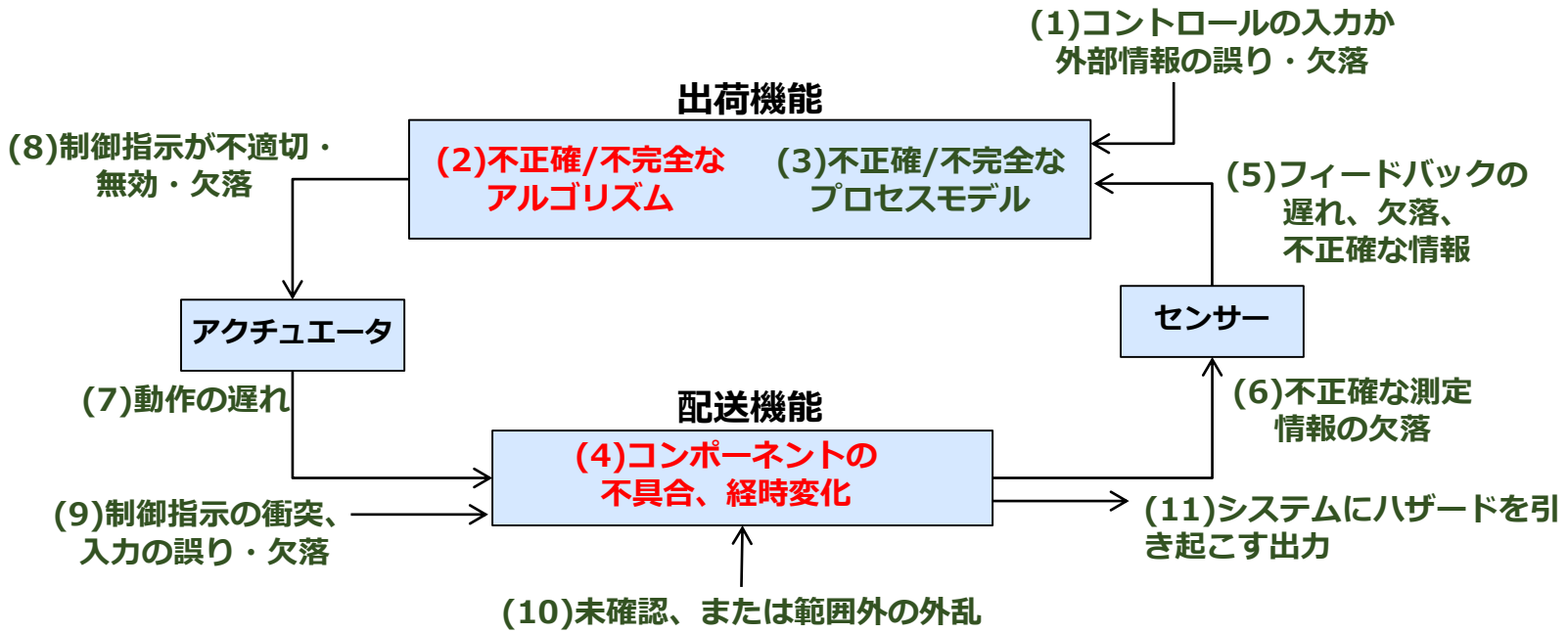
- **UCA5：「出荷指示が発行されたが、ピックアップ・出荷が行われない」**
  Request for shipment is provided, but shipment is not provided.

⇒ 考えられる原因： Cause of the UCA

- 担当者が出荷指示を見落とす　Request for shipment is overlooked.
- 配送者(車)が配送中のため出荷できない　Delivery person is not there. (all gone for delivery)

⇒ 導かれる安全要件： Safety Requirement

- 出荷指示が確実に認識されること　Request for shipment should be surely recognized.
- 十分な数量の配送者(車)が配備されていること　Enough number of delivery person should be allocated.



(5) UCAの原因の識別
Identifying the causes of the UCAs

SEC Software Reliability Enhancement Center

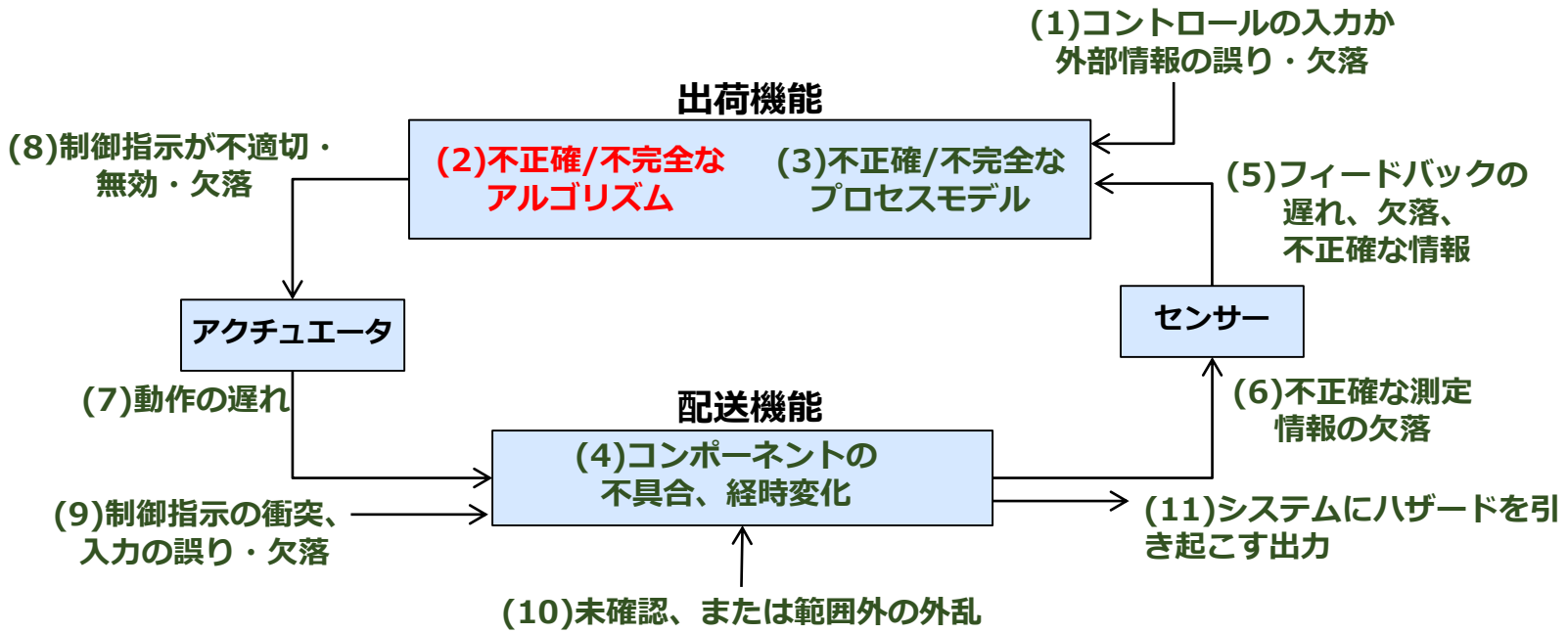
- **UCA6：「出荷指示と異なる商品がピックアップ・出荷される」**
  Incorrect product is shipped.

⇒ **考えられる原因：** Cause of the UCA

・担当者が出荷指示を誤認する　Misunderstanding of request for shipment.

⇒ **導かれる安全要件：** Safety Requirement

・出荷指示が確実に認識されること　Request for shipment should be correctly recognized.



STPA分析結果のまとめ
Results of STPA analysis

SEC Software Reliability Enhancement Center

UCA	原因 Cause	安全要件 Safety requirement
(UCA3) 在庫が無い状況で出荷指示が発行される	在庫データ更新の遅延または欠落のため、在庫数が不正となり、在庫が無い状況で「引当て可」が通知される	商品の引当てを行う前に在庫データの更新が完了していること。 対策例：「商品の引当て」処理の事前条件として、データ更新済みであることを加える。
(UCA5) 出荷指示が発行されたが、ピックアップ・出荷が行われない	担当者が出荷指示を見落とす	出荷指示が確実に認識されること 対策例：出荷指示を認識したことを販売管理にフィードバックする。販売管理はフィードバックが無ければ再指示する。
	配送者(車)が配送中のため出荷できない	十分な数量の配送者(車)が配備されていること 対策例：最大受注量を見積もり、配送者(車)の数量を決定する。
(UCA6) 出荷指示と異なる商品がピックアップ・出荷される	担当者が出荷指示を誤認する	出荷指示が確実に認識されること 対策例：出荷指示の認識内容を販売管理にフィードバックする。販売管理はフィードバックに誤りがあれば再指示する。

現時点の個人的な考察
Discussion

SEC Software Reliability Enhancement Center

- 業務系システムに対してSTPA分析の手法は適用可能か
  Is STPA applicable to enterprise systems?
  - 業務系では仕様がデータ処理の観点で表現され、制御が明示的でないことが多い。
    In enterprise systems, specification is usually expressed in terms of data processing, and “control” is not explicitly expressed, which makes creating control structure not easy.
  - しかし、ハザードに関わる処理（アクション）は存在し、それらのアクションをSTAMPの制御構造モデルで表現することは可能。
    But, “actions” that can affect the safety requirements surely exists in Activity Diagram, and from such actions, it was possible to create control structure.
  - STPAの手順適用により、例題の業務仕様に欠けていた安全要件を導出できた。
    By applying STPA, we could identify safety requirements which were not in the initial specification.

- 業務系にSTPAを適用する場合の特徴的な点
  Any features specific to applying STPA to enterprise systems?
  - UCAの識別やHCFの分析では、データの流れを示す仕様を参照すると分かりやすい。
    Referring activity diagram (which shows data flow) made it easier to identify UCAs and cause of the UCAs.
  - これは、コントロールアクションが、大域的なデータ（データベース）に依存することが多いためだと考えられる。
    This would be because most of control actions depend on “global data (database)” which can be updated by many other actions, and without such information, it is difficult to imagine hazard scenario.

まとめ

- IPA/SECのWGで調査を進めている業務系システムへのSTPA分析の応用検討について報告
- 例題とした通販システムの事故は「許容できない損失」としてのリアリティに乏しかったかもしれないが、STPA分析により安全要件を導くプロセスを確認できた
- 業務系システムにおけるSTPA活用の可能性を示す実験として価値があると思われるため、今後も継続してWGで検討予定


IPA
Better Life
with IT