RENTACO

第3回STAMPワークショップ資料

業務プロセスにSTPA手法を適用する試み
～システム化の要求を導出するために～

2018年12月3日
JASA　安全仕様化WG　主査
株式会社ジェーエフピー　顧問
中村　洋

はじめに

◆背景

- JASA安全仕様化WGは、制御システムに関してSTAMP/STPA手法を用いたハザード分析を試みてきた。
- 業務システムに関しては、要求定義の不備に起因するシステム障害が依然として多い。システム化の対象となる業務プロセスを分析し、障害要因を事前に摘出できれば、有効な解決策となる。
- しかし、業務プロセスに適用する方法論はまだ整備されていない。

◆目的

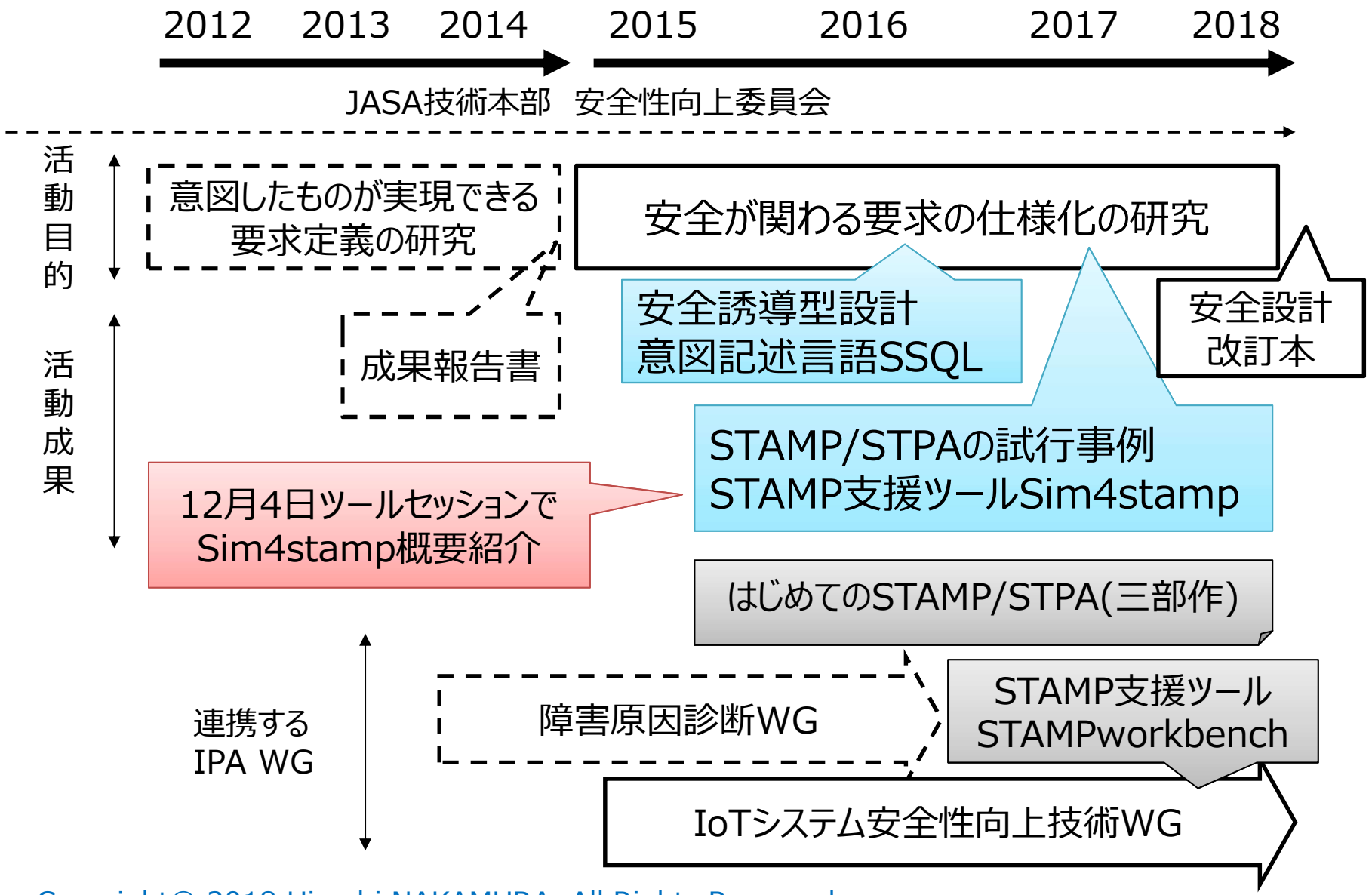
- 業務プロセスへSTPA手法を適用して、システム開発に関する要求事項を導出する方法論を考察すること。

◆実施方法

- 卸売業の販売プロセスを題材にする。
- 業務プロセスがハザードを引き起こすかをSTPA手法で分析する。
- 詳細化された安全制約からシステム化の要求事項を導出する。

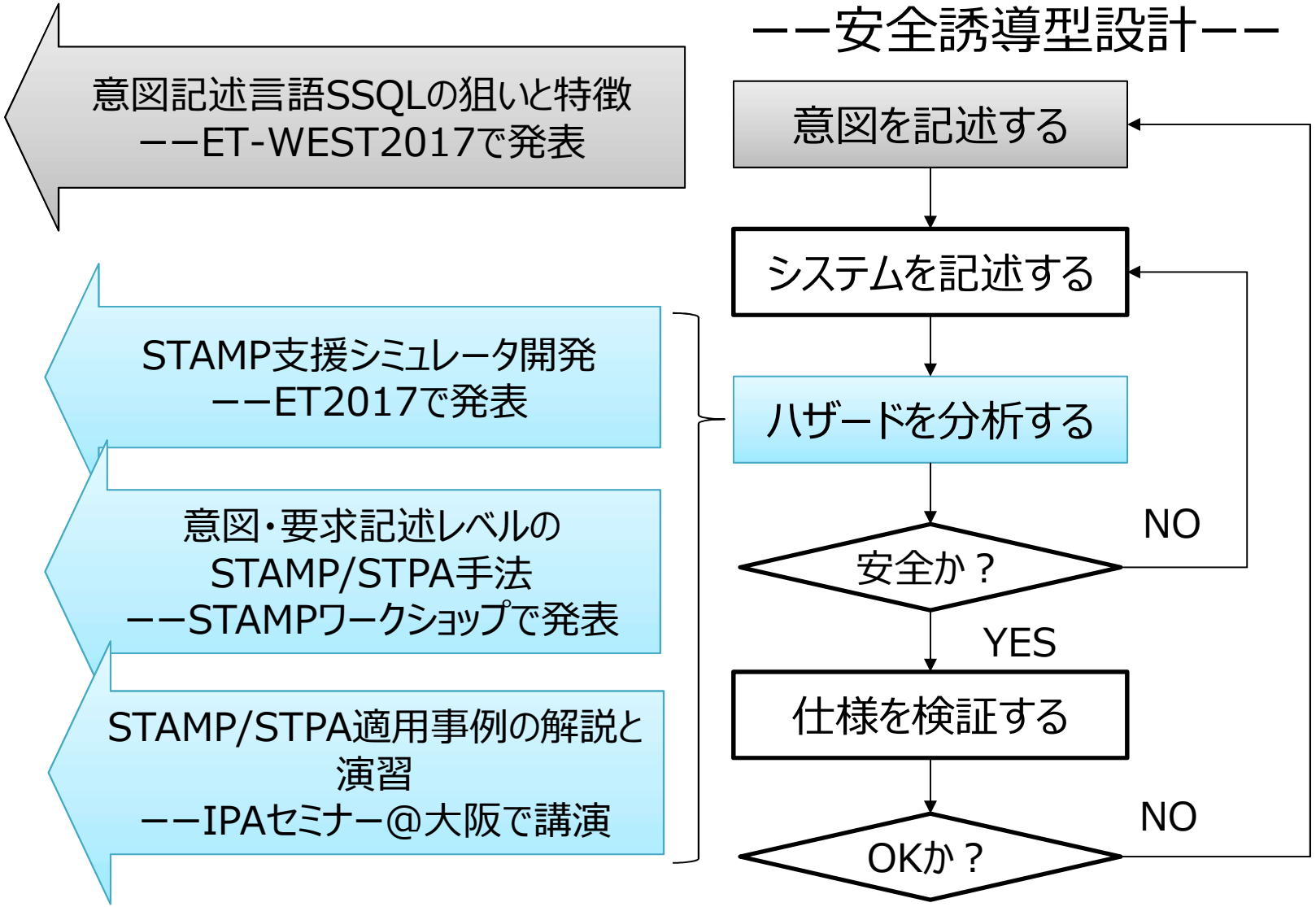
RENTACO

安全仕様化WG：その活動推移



RENTACO

プロセスモデルに対応する活動成果



RENTACO

題材：卸売業

◆業務プロセス
- ■ 販売プロセス
- ■ 購買・在庫管理プロセス
- ■ 経理・財務プロセス
- ■ 人事プロセス

◆業務組織
- ■ 営業、営業管理
- ■ 倉庫
- ■ 購買物流
- ■ 経理・財務、審査
- ■ 人事・法務・総務

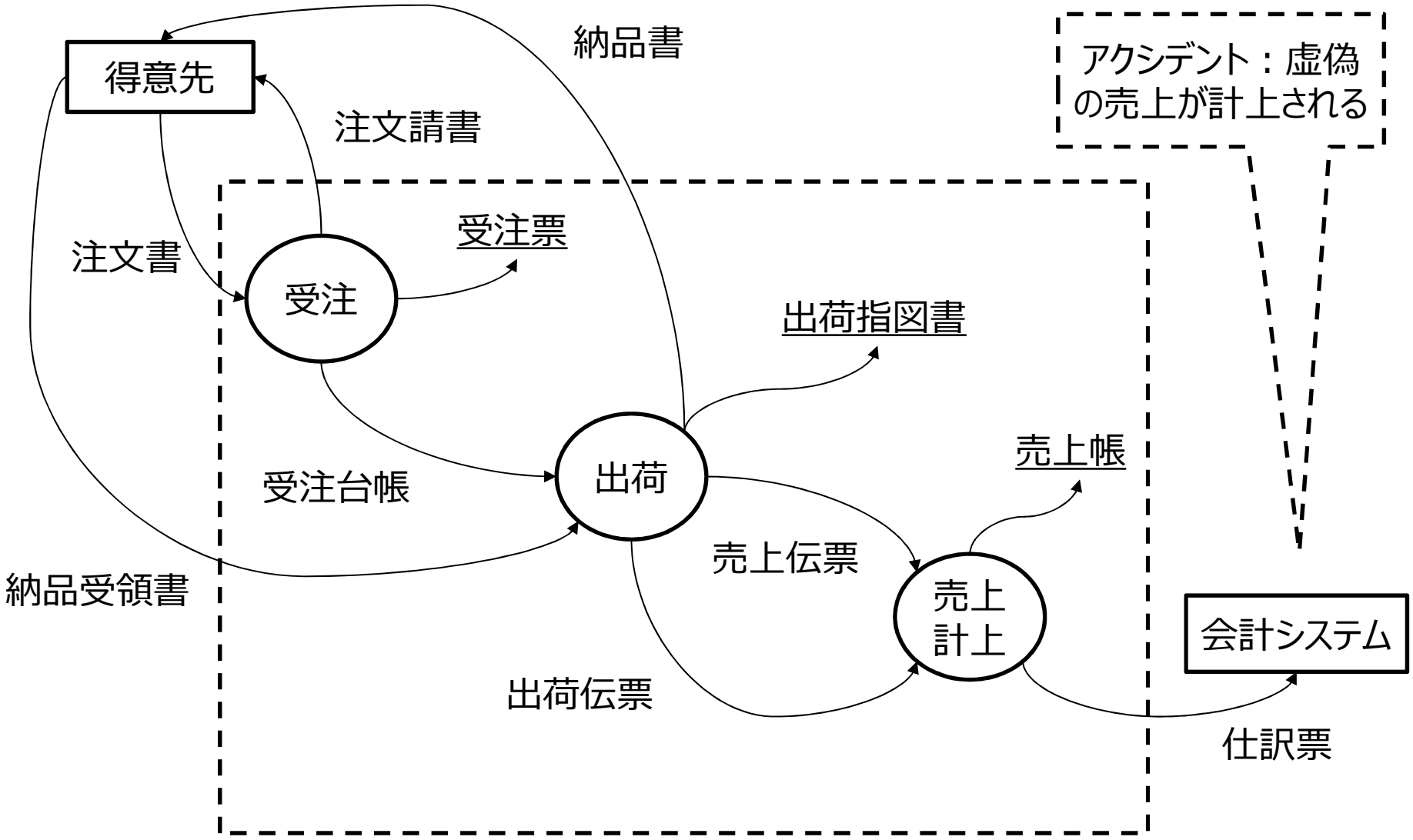
- ◆ SA1　与信管理
- ◆ SA2　受注
- ◆ SA3　出荷
- ◆ SA4　売上計上
- ◆ SA5　請求書発行
- ◆ SA6　入金
- ◆ SA7　返品
- ◆ SA8　売掛金残高管理
- ◆ SA9　貸倒処理
- ◆ SA10　貸倒引当金の設定

BPM図

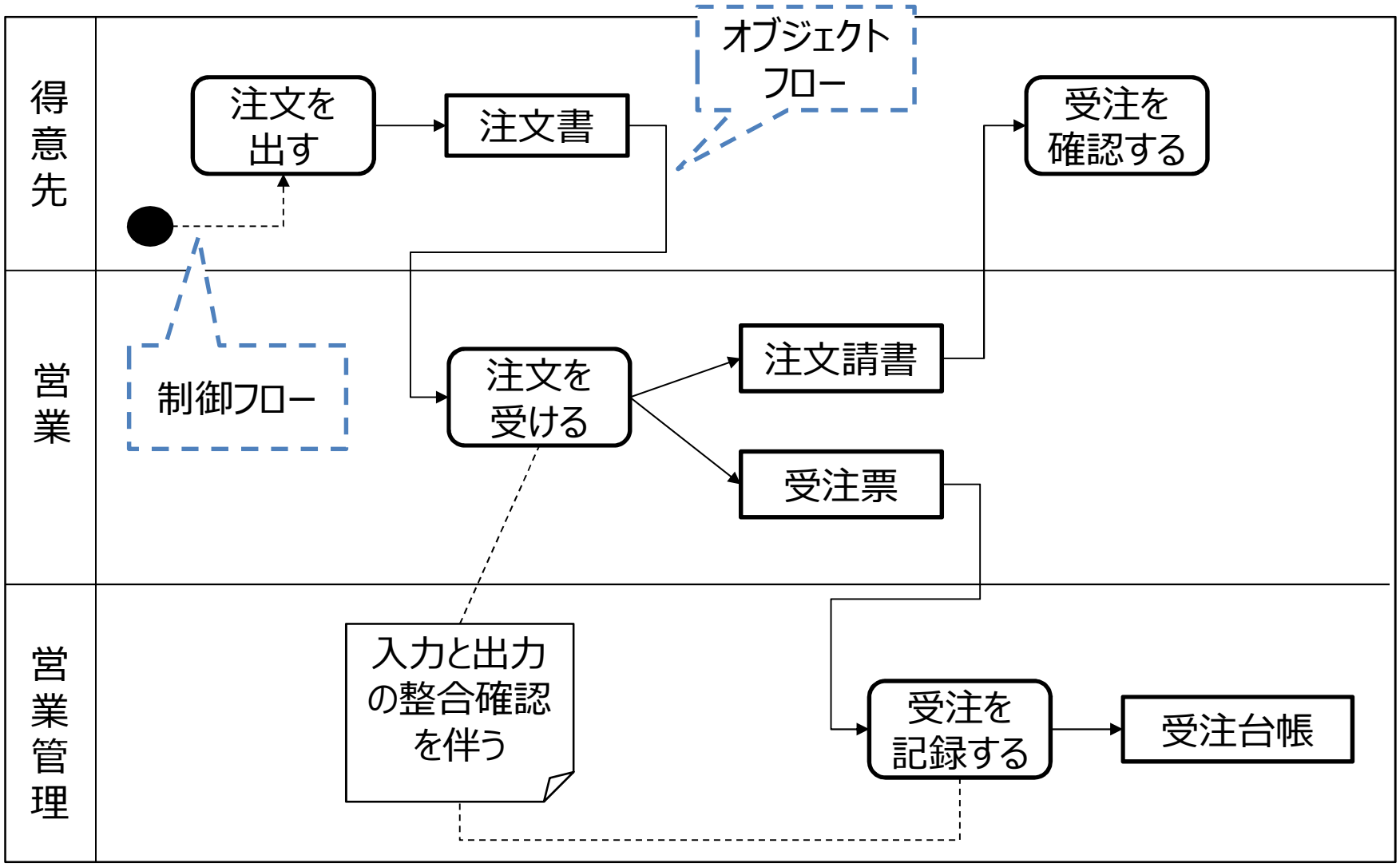
- ◆ PA1　新規取引
- ◆ PA2　発注
- ◆ PA3　入荷・検収
- ◆ PA4　仕入計上　（SA4に同じ）
- ◆ PA5　請求書照合
- ◆ PA6　返品
- ◆ PA7　買掛金残高管理　（SA8に同じ）
- ◆ PA8　在庫残高管理
- ◆ PA9　在庫の廃棄処理

RENTACO

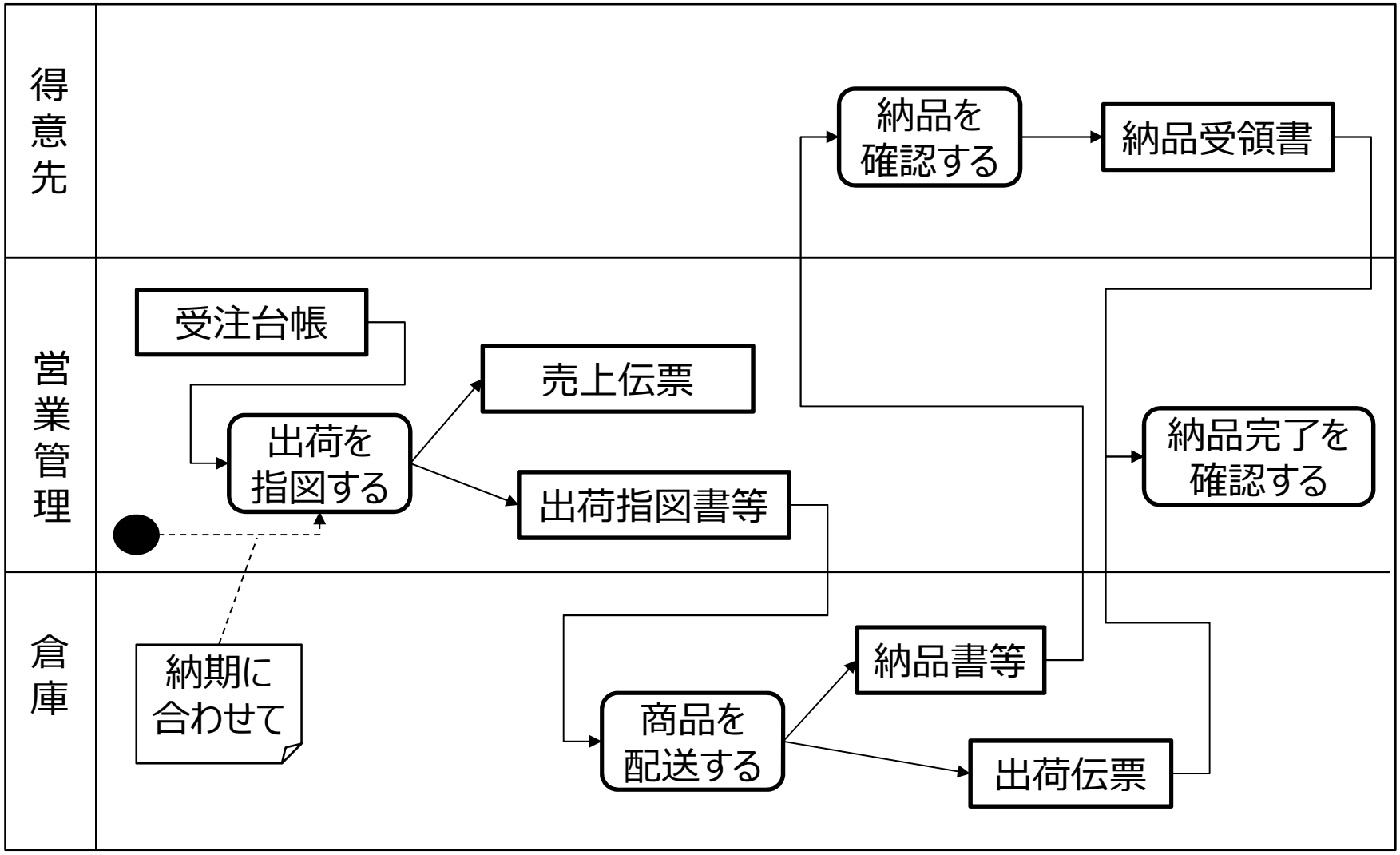
分析対象：受注から売上計上まで



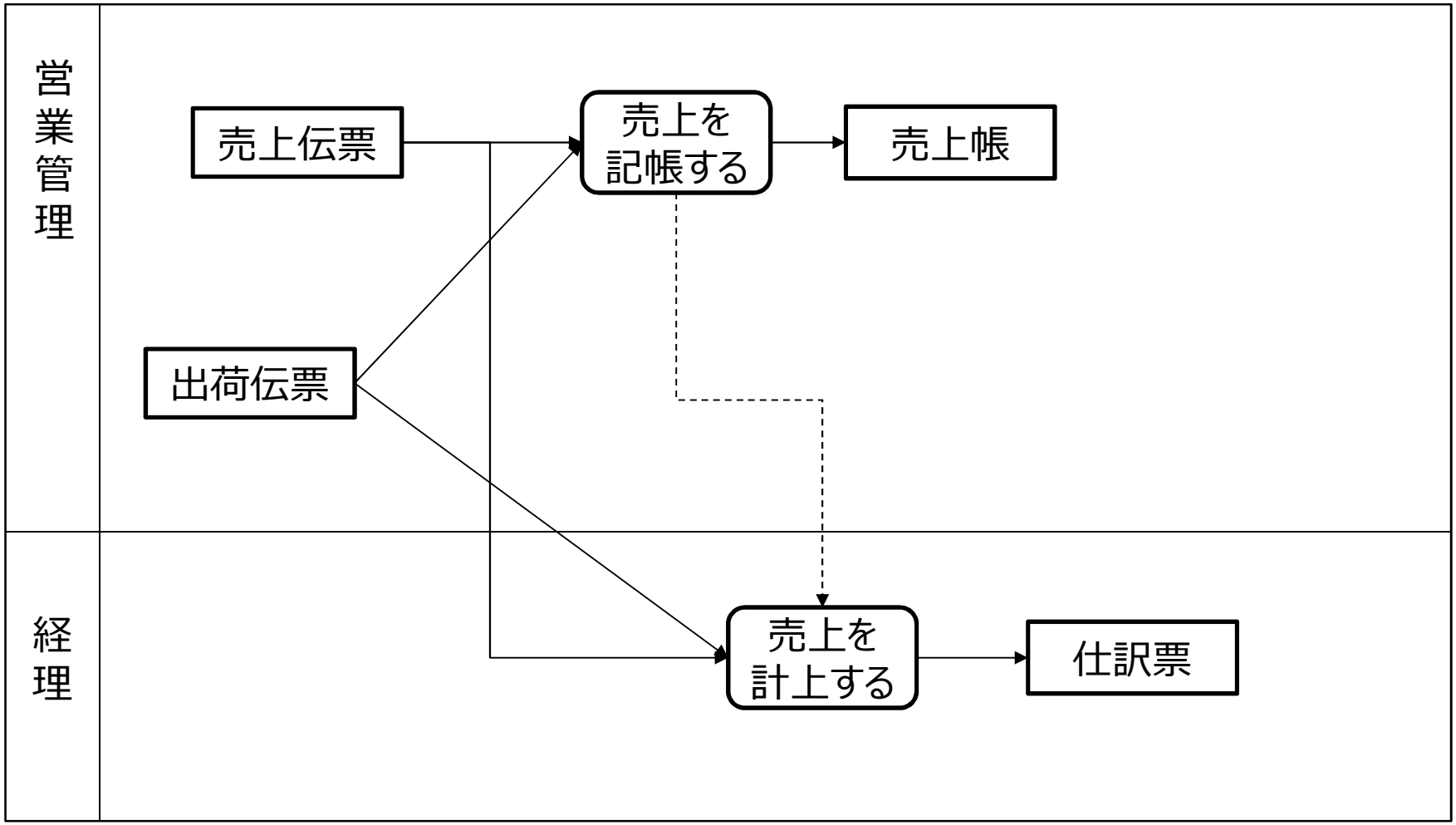
受注



出荷



売上計上



各部署の責務

プロセス 部署	受注	出荷	売上計上
得意先	意図する注文書を作成し、注文請書を受けてそれを確認する。	納品された商品が注文に一致することを確認する。	
営業	注文書に整合する受注票と注文請書を作成する。		
営業管理	受注票に整合するように、受注台帳に受注を記録する。	納期に合わせて受注台帳に整合する売上伝票、出荷指図書、納品書、納品受領書を作成し、得意先からの納品受領書を受けて納品完了を確認する。	出荷伝票を受けて、売上帳に売上を記録する。
倉庫		出荷指図書に従って納品書等を得意先に配送し、出荷伝票を作成する。	
経理			売上伝票、出荷伝票に整合する仕訳票を作成する。

業務プロセスにSTPA手法を適用する手順

1. 業務プロセスを理解する
   - アクティビティ図やデータフロー図等の標準的な記法を用いて、分析対象となる業務プロセスを記述する。
2. アクシデント、ハザード、安全制約を識別する
3. 業務プロセスを反映する制御構造を描く
   - 業務プロセスにおける部署をコンポーネントとする。
   - 他部署に文書を渡し指示する作業が制御行動に、指示された作業の結果を伝える作業がフィードバックに、それぞれ対応させる。
4. ハザードを引き起こす恐れのある制御行動を識別する
   - 過失や故意によってUCAを引き起こす状況や条件を考える。
5. 業務プロセスに関わるハザード誘発要因を識別する
   - 業務の流れに沿ってハザードに至るシナリオを見つける。
6. システム化の要求事項を導出する
   - ハザードシナリオを回避するため、安全制約を詳細化、具体化する。

識別されたアクシデント、ハザード、安全制約

◆アクシデント

■ 虚偽の売上が計上される

ハザード:
特定の最悪な環境条件と重なって、
事故(損失)を引き起こす
システム状態又は条件

◆ハザード

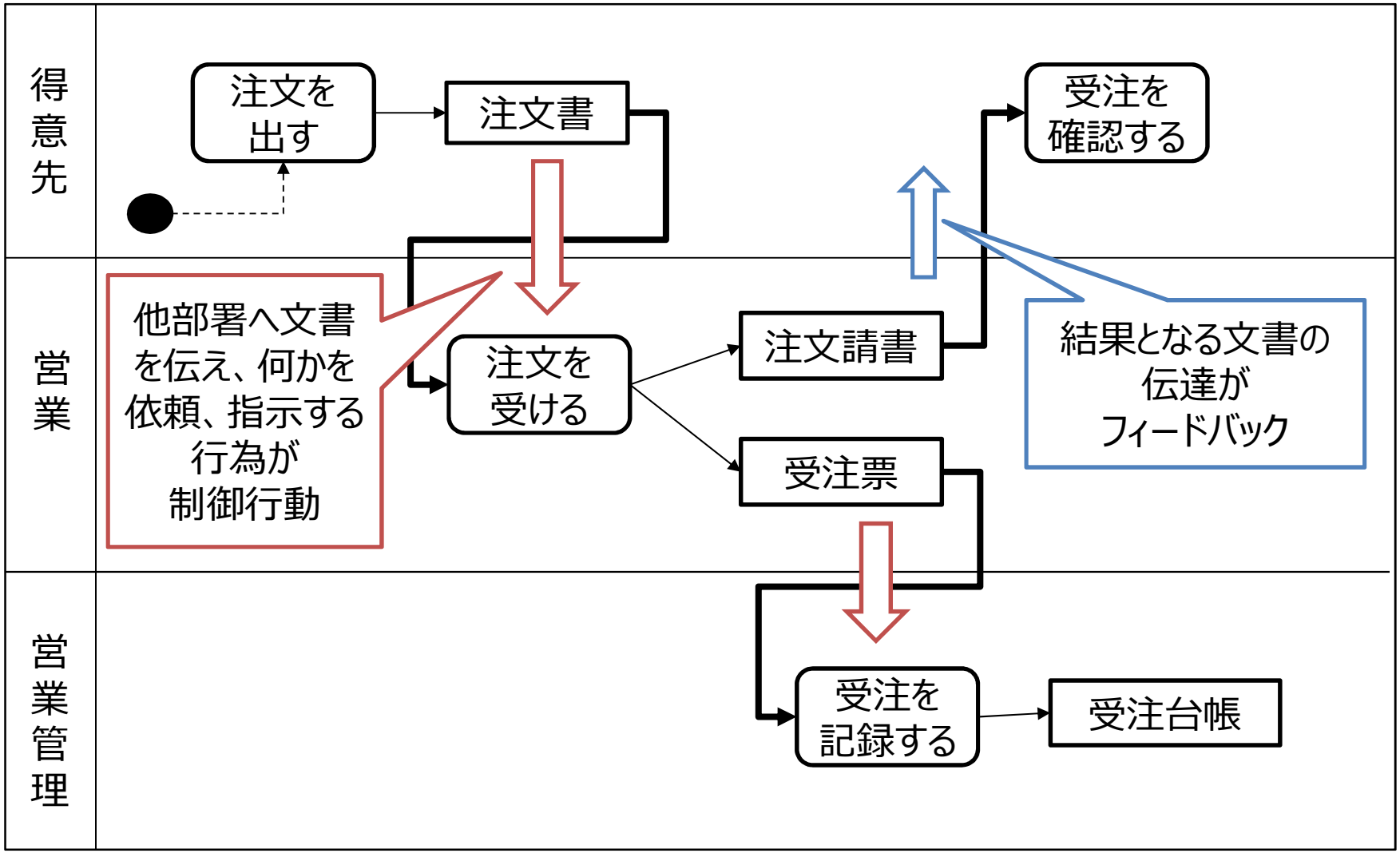
■ 虚偽記載が検出されない（文書間の不整合が検出されない）

◆安全制約

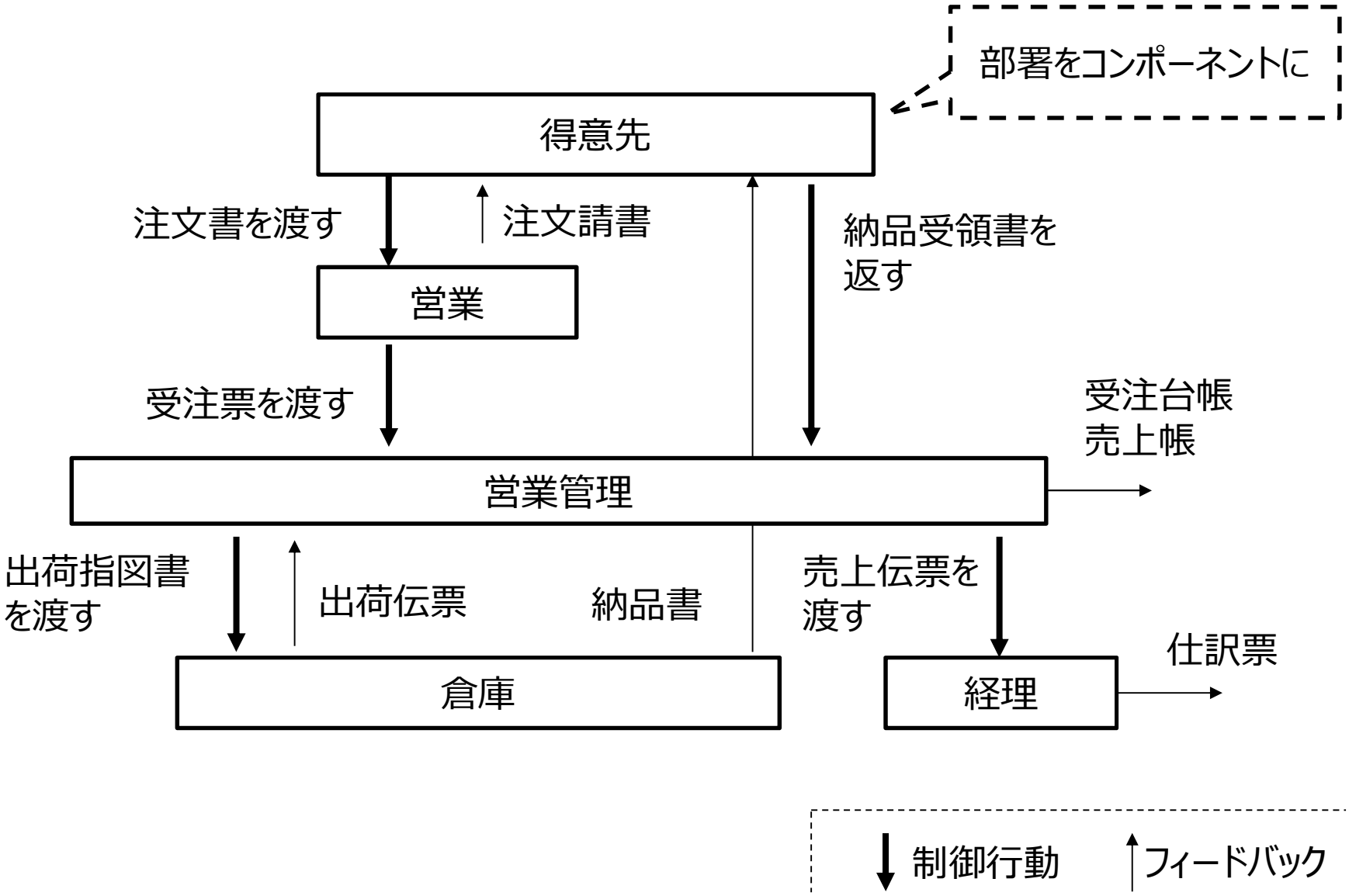
■ 過失又は故意による虚偽記載を防止又は検出する

RENTACO

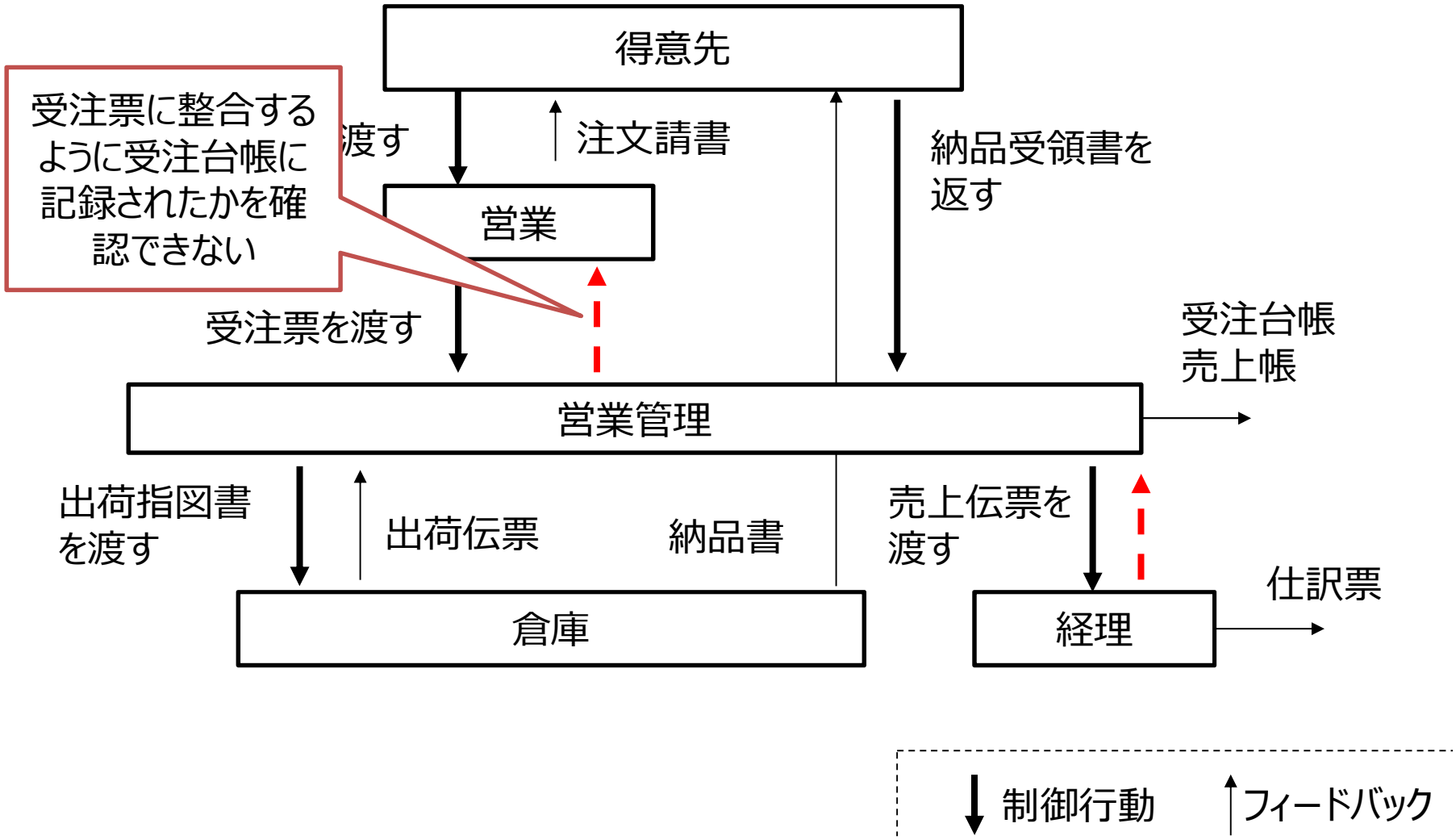
課題：何が制御行動で、何がフィードバックか？



制御構造図



気づくこと：フィードバックの欠如



UCA識別表の変更：UCAの3パターン

ガイドワードの順序を変更

制御行動	与えられないとハザード(N)	早すぎ、遅すぎ、誤順序でハザード(T)	早すぎる停止、長すぎる適用でハザード(D)	与えられるとハザード(P)
注文書を渡す	N/A	UCA1-P1：偽の注文書を渡す。 UCA1-P2：注文書に整合しない受注票が作成される。		
受注票を渡す	注文された商品が届かない。	UCA2-T1：注文書との整合が確認される前に受注票を渡す。 UCA2-P1：ねつ造した受注票を渡す。 UCA2-P2：受注票に整合しない受注が受注台帳に記録される。		

先行作業の省略

与える側のねつ造行為

与えられる側の不整合行為
（フィードバック欠如）

UCAの識別

制御行動	与えられないとハザード(N)	早すぎ、遅すぎ、誤順序でハザード(T)	早すぎる停止、長すぎる適用でハザード(D)	与えられるとハザード(P)
注文書を渡す	N/A	UCA1-P1：偽の注文書を渡す。 UCA1-P2：注文書に整合しない受注票が作成される。		
受注票を渡す	注文された商品が届かない。	UCA2-T1：注文書との整合が確認される前に受注票を渡す。 UCA2-P1：ねつ造した受注票を渡す。 UCA2-P2：受注票に整合しない受注が受注台帳に記録される。		
出荷指図書を渡す	納期が来ても注文された商品が届かない。	UCA3-T1：整合が確認される前に出荷指図書を渡す。 UCA3-P1：ねつ造した出荷指図書を渡す。		
売上伝票を渡す	売上が計上されない。	UCA4-T1：出荷伝票が届く前に、売上伝票と偽装された出荷伝票を渡す。 UCA4-P1：ねつ造した売上伝票を渡す。 UCA4-P2：売上伝票と出荷伝票に整合しない仕訳票が作成される。		
納品受領書を返す	納品完了を確認できないが、出荷基準なので売り上げは計上される。	N/A		

ハザードシナリオ：UCA1に関して

UCA	シナリオ	安全制約
UCA1-P1：偽の注文書を送付する	1. 得意先になりすました者が、注文書を送付する。 2. 営業は、偽の注文書をもとに受注票と注文請書を作成する。 3. 受注票と注文請書を注文書と照合する。 4. 営業は整合確認済みの注文請書を得意先に返送する。 5. なりすまし者はその注文請書を無視する。	偽の得意先からの注文を検出する。
UCA1-P2：注文書に整合しない受注票が作成される	1. 営業は、故意に注文書と異なる受注票を作成する。 2. 自ら注文書との整合確認を行う。 3. 注文書と整合する注文請書を得意先に送付する。 4. 受注票の虚偽記載が検出されない。	同じ人が文書作成と整合確認を行ってはならない。

業務プロセスに関する記述に基づく、ハザードに至る業務の流れ

ハザードを引き起こさないための、詳細化、具体化された安全制約

ハザードシナリオ：UCA2に関して

UCA	シナリオ	安全制約
UCA2-T1：注文書との整合が確認される前に受注票を渡す	1. 営業は、注文書をもとに受注票を作成する。 2. 急いでいたので、注文書との整合確認を省く。 3. 受注票が注文書とは異なることが検出されずに、それを営業管理に渡す。	整合確認ができていない文書を検出する。
UCA2-P1：ねつ造した受注票を渡す	1. 営業は、注文書をもとに受注票を作成する。 2. 注文書との整合が確認される。 3. 整合確認済みの受注票を偽装し、それを営業管理に渡す	改ざんされた整合確認済みの文書を検出する。
UCA2-P2：受注票に整合しない受注が受注台帳に記録される	1. 営業は、整合確認済みの受注票を営業管理に渡す。 2. 営業管理は、それを無視して、受取ったものとは異なる受注を受注台帳に記録する。	営業は、受注台帳が受注票に整合することを確認する。
	1. 営業は、整合確認済みの受注票を営業管理に渡す。 2. 営業管理は、ついうっかり、受取ったものとは異なる受注を受注台帳に記録する。 3. 同一人物が受注票との照合を行い、不整合が検出されない。	UCA1-P2に同じ

UCA3とUCA4は省略

導出されたシステム化の要求事項

◆業務プロセスに関して

- 同じ人が文書作成と整合確認を行ってはならない。
- 営業は、受注台帳が受注票に整合することを確認する。
- 営業管理は、売上伝票と、出荷伝票、仕訳票が、受注台帳に整合することを確認する。（UCA4-P2から導出）

◆技術的課題として

- 偽の得意先からの注文を検出する。
- 整合確認を実施していない文書を検出する。
- 改ざんされた整合確認済みの文書を検出する。

システム化の対象となる業務プロセスにSTPAを適用して、
システム開発の要求事項を導出することができた

考察

◆業務プロセスから制御構造を描けるか？
- ■ 他部署に文書を渡し、依頼又は指示する作業が制御行動。
  - ●その結果となる文書の伝達はフィードバック。
- ■ すべてのデータフローを分析する手法に比べて、絞り込みが可能。

◆非安全な制御行動を識別できるか？
- ■「早すぎ、」、「早すぎる停止、」、「与えられる」の順で。
  - ●「早すぎ、」：先行作業の省略
  - ●「早すぎる停止、」：N/A
  - ●「与えられる」：与える側のねつ造、与えられる側の不整合行為
- ■ ガイドに従って系統的な分析が可能。

◆STPA手法は業務システム開発に使えるのか？
- ■ 業務プロセスに対する定型化されたリスク分析手法として使える。
- ■ 分析結果からシステム化の要求事項を導出できる。
- ■ 業務知識のプロなら、もっと成果を出せるはず。

さあ、「業務プロセスへのSTPA適用」にトライ！！

問合せ先：
中村　洋
hiroshi19.nakamura@nifty.com