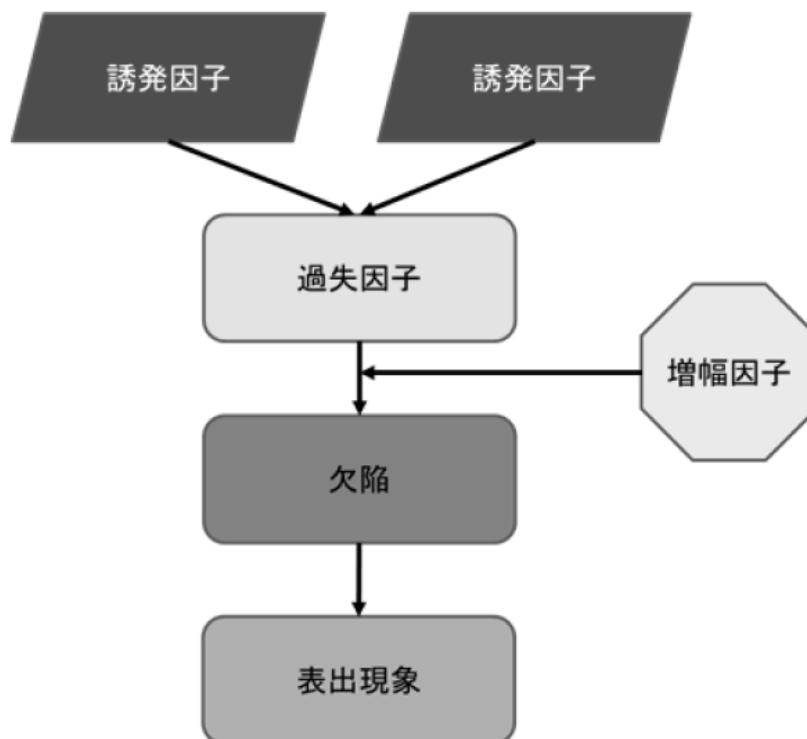


付録 1. 欠陥モデル(Defect model)の定義

<要素の定義>

要素	要素の説明
誘発因子 (Induction Trigger)	成果物の中に含まれる，人間の思考の誤りを誘発する“トリガー”となる要素のこと。 誘発因子が存在すれば，開発者能力・経験・技術力と関係なく過失が引き起こされやすくなる。
過失因子 (Negligence Factor)	人間の思考や判断の誤りそのもののこと。 欠陥は過失因子の集合（＝連続）として生み出される。
増幅因子 (Amplifier)	過失の連鎖を助長し，欠陥の混入確率を増幅させる要素。 多くは定量的に計測可能である．外乱・環境特性ともいう。
欠陥 (Defect)	成果物に含まれた，人間の思考の過ちが具現・表出化したもの。 不具合・障害等の”現象”を発生させる。
表出現象 (Incident)	欠陥によって引き起こされる不具合・障害。 多くは定量的に計測／加算可能。

<モデル構造>



付録 2. MARS (Multi-Attribute Representation of Software defect) モデルの作成手順

MARS モデルの作成手順は以下のとおりである。

- (1) 欠陥情報のインプットとしてアブストラクションシート（付録 4 に実例）を作成する。

アブストラクションシートとは，発生事象，原因（混入原因，未検出原因，発症原因），対策，記述の抽象度を記録するものである。

- (2) アブストラクションシートから多属性表現（MASR モデルの基本の 5 属性）で欠陥自体を表現

特性，位置，種類，正常／異常，経年という軸で，欠陥表を分割する。

特性	対象・位置	種類	正常／異常	経年
24 時間運転が基本 当該処理自体の変更なし	起動タイミング	例外処理抜け	異常系	Y E S (他機能の改修)

※MARS モデルから Z-Chart の作成について

MARS モデル（多属性表現した欠陥）から FM (Failure Mode：故障モード) の連続として欠陥を表現する。

MARS モデルを利用し，Z-Chart ヘトリガーから順番に，誘発因子，思考（過失），現象（欠陥）を追記することで，各行を FM として蓄積することができる。

	トリガー	誘発因子	思考（過失）	現象（欠陥）
FM1-1	システム改修	システムを再起動	工場で試験を完了しているので問題ない	工場と現地では蓄積データに差異がある
FM1-2	蓄積データに差異がある	今回の改修に伴うデータは，現地から入手して試験を実施	改修部分の試験は現地データを用いて実施したので問題ない	改修部ではなく再起動という現地作業に問題
FM1-3	現地作業における問題	現地と工場ですべて同一な環境を作るのは困難	工場ですべて実施した	データ初期化処理が再起動中に動作せず

付録 3. MARS モデル作成におけるポイント

<各属性抽出時のポイント>

作成手順のポイント

- ・ MARS モデルを作成する場合,

- ① 自由に記述する欠陥の” 特性”
- ② 排他的属性である” 正常／異常” , ” 経年”
- ③ 故障モードに近い” 位置” , ” 種類”

の順で作成し, その上でモデルを膨らませる形で作成を行うと比較的作成しやすい.

各属性を考える際のポイント

- ・ ” 特性” については, 欠陥の特徴を示す性質を記述するものであるため, 欠陥情報の内, ポイントとなるキーワードを見つけてから考えると書きやすい.
※” 特性” を考える際に欠陥情報からキーワードを見つけることとなるが, キーワードについては, ” テキストマイニング” を使うと候補を洗い出すことが可能であると考えられるため, ある程度の自動化も可能であると考えられる.
- ・ “正常／異常” , ” 経年” は, その欠陥での一番の” 特性” に対して, 考えると判断がしやすい
- ・ ” 位置” , ” 種類” は, 一度, 考えて思いつかない場合には, ” 特性” , “正常／異常” , ” 経年” の 3 つの情報から考えると, 比較の出しやすい

MARS モデルの各属性の詳細 (再掲+補足)

属性	詳細
特性	欠陥を示す特徴的な性質 (例: 単独では起こらない) 補足) 欠陥が起こる際に必要となる性質や, 対象欠陥固有の特徴を指している
位置	欠陥の原因の位置 (例: I/F) 補足) 表出現象が起こる原因となっている箇所を指している
種類	欠陥が発現した原因の種類 (例: 齟齬) 補足) 欠陥を誘発したものの抽象度を上げたものを指している
正常／異常	欠陥が正常系の動作で発生するか, 異常系の動作で発生をするか (正常/異常)
経年	時間が経過による変化が欠陥に関連するか否か (Yes/No)

利用しやすいモデルを作成するポイント

- ・ 思考の流れを矢印で細かく示すと作成者の思考の流れをモデル利用者に伝えることができるようになり, 伝えたい情報の意図が伝わりやすくなる.

MARS モデルの例（再掲）

特性	対象・位置	種類	正常／異常	経年
単独では起こらない	I/F	齟齬 ↓ 例外処理	異常	No (当初想定の使用 方法範囲内)
入力の正常／ 異常ケースの 区分別に漏れ				

↓
 バグ：アプリケーションが停止しない
 ↓
 結果：（While）無限ループ

付録 4. 実験で使⽤した欠陥情報

実験では、＜欠陥情報＞、＜欠陥モデリング”でのモデル表現＞、＜ソフトウェア欠陥の多属性表現（MARS モデル）＞を以下の表現で提示した。グループ A では、同じ人が欠陥モデルを始めに参照し、そこから想起できる欠陥を洗い出し、次に MARS モデルを参照し、追加で想起できる欠陥を洗い出した。具体的に提示したものを付録 6 に示す。ただし、アブストラクションシートは、本付録では省略した。

＜欠陥情報＞

対象：入力文字列と画像内の文字列を比較するアプリケーション

アブストラクションシート（各要素の詳細については、付録 5 を参照）

タイトル		空白文字，空白行入力時のアプリケーションの無限ループ
発生事象		空文字列もしくは，空白行（改行のみもしくは，改行+空白のみ入力）が含まれる文字列を入力した場合に，アプリケーションが停止しない現象が発生する
実害		アプリケーションが停止しない
抽象度		Mid
原因	混入原因	規定されていた入力に対する While ループの停止条件は正しく設定されていたが，異常値入力時の考慮が不足していた.
	未検出原因	DB とアプリを統合後のテストにおいて，規定された入力以外のテストがされていなかった.
	発症原因	異常値である空白文字，空白行が DB にあり，発症
関連		追加要望）スペース，空白行を加味したアプリケーションに改修のこと
対策		空文字列，スペース，空白行を許容する形に再設計

“欠陥モデリング”でのモデル表現

誘発因子	対象箇所への入力とは別で作成された DB を利用（自動入力）	While ループ停止条件の付け方ルールが明確となっていなかった
増幅因子	DB とアプリ間での整合不足 チェック体制不備	コーディングルールの不備
過失因子	空文字列、空白行が入力されること想定されていなかった ※DB への登録段階で削除を想定	設計者の思い込み
欠陥	While ループ停止条件に漏れあり、入力が空（空白文字、空白行あり）の場合に While ループが無限ループとなる ※例外動作が定義されていない	
表出現象	アプリケーションが停止しない	

ソフトウェア欠陥の多属性表現（MARS モデル）

特性	対象・位置	種類	正常／異常	経年
単独では起こらない	I/F	齟齬 ↓ 例外処理	異常	No (当初想定の使用 方法範囲内)
入力の正常／異常ケースの区判別に漏れ				

↓
バグ：アプリケーションが停止しない
↓
結果：（While）無限ループ

※補足情報

故障モード：ソフトウェアが本来より（動作が）多い

種類：無限ループ

位置：ループ制御部（機能主要部）

過失因子：（ループ制御部の）例外動作の定義忘れ

入力部の想定漏れ

（DB と入力部の）仕様整合漏れ

誘発因子：部署間（DB 作成部署と入力部作成部署）の連携不備

開発段階で運用時の DB との統合テストができる環境がなかった

付録 5. アブストラクションシートの定義

<要素の定義>

要素	要素の説明
タイトル	伝えたい内容を簡潔に伝えることができるタイトルを記入
発生事象	欠陥に起因して発生した事象を記入
実害	発生事象により実際にもたらされた害を記入
抽象度	各要素での記入内容の抽象度を記入 【抽象度】 Min：抽象化は行っていない（関係者内で公開レベル） Mid：関係者以外に公開可能なレベルまで抽象化がされている Max：組織外に公開可能なレベルまで抽象化がされている
原因－混入原因	欠陥が混入した原因を記入
原因－未検出原因	欠陥が表出するまで検出できなかった原因を記入
原因－発症原因	欠陥が表出した原因を記入
関連	関連する欠陥モデル，アブストラクションシートを記入
対策	欠陥の再発防止，混入防止の対策を記入

付録 6. 実験で提供したモデル (8 欠陥)

No. 1 : 入力文字列と画像内の文字列を比較するアプリケーション

誘発因子	対象箇所への入力とは別で作成された DB を利用 (自動入力)	While ループ停止条件の付け方ルールが明確となっていなかった
増幅因子	DB とアプリ間での整合不足 チェック体制不備	コーディングルールの不備
過失因子	空文字列, 空白行が入力されること想定されていなかった ※DB への登録段階で削除を想定	設計者の思い込み
欠陥	While ループ停止条件に漏れあり, 入力が空 (空白文字, 空白行あり) の場合に While ループが無限ループとなる ※例外動作が定義されていない	
表出現象	アプリケーションが停止しない	

ソフトウェア欠陥の多属性表現 (MARS モデル)

故障モード: ソフトウェアが本来より (動作が) 多い

種類: 無限ループ

位置: ループ制御部 (機能主要部)

過失因子: (ループ制御部の) 例外動作の定義忘れ

入力部の想定漏れ (DB と入力部の) 仕様整合漏れ

誘発因子: 部署間 (DB 作成部署と入力部作成部署) の連携不備

開発段階で運用時の DB との統合テストができる環境がなかった

Type : FMEA 分類 (ソフトウェア欠陥の多属性表現)

特性	位置	種類	正常/異常	経年
単独では起こらない	I/F	齟齬	異常	No (当初想定の使用 方法範囲内)
入力の正常/ 異常ケースの 区分別に漏れ		例外処理		

↓
バグ: アプリケーションが停止しない

↓
結果: (While) 無限ループ

仕様整合漏れ

過失とも見える

誘発

過失

No. 2：入力文字列と画像内の文字列を比較するアプリケーション

誘発因子	他社製関数の制約条件の調査方法が明確になっていなかった	制約条件を理解するのに必要な高度な画像認識の知識が不足していた (教育不足)
増幅因子	制約条件の調査時間を確保できていなかった テストが不十分	
過失因子	制約条件に抵触していることを認識していなかった (制約条件の理解不足)	
欠陥	他社製関数の制約条件下での動作へのケアがされておらず、特定オブジェクトの検出がされない状態となっている(関数が正常に動作していない)	
表出現象	対象画像内にある特定のオブジェクト(表示)を検出することができない ⇒検出され、その検出位置が出力されるはずが、出力されない	

ソフトウェア欠陥の多属性表現 (MARS モデル)

故障モード：アクセス方法が異常(制約条件下に抵触しているにも関わらず、アクセスしている)

種類：外部(関数への)アクセス不備

位置：外部(関数との)連携部

過失因子：外部(関数)の制約条件の確認不足

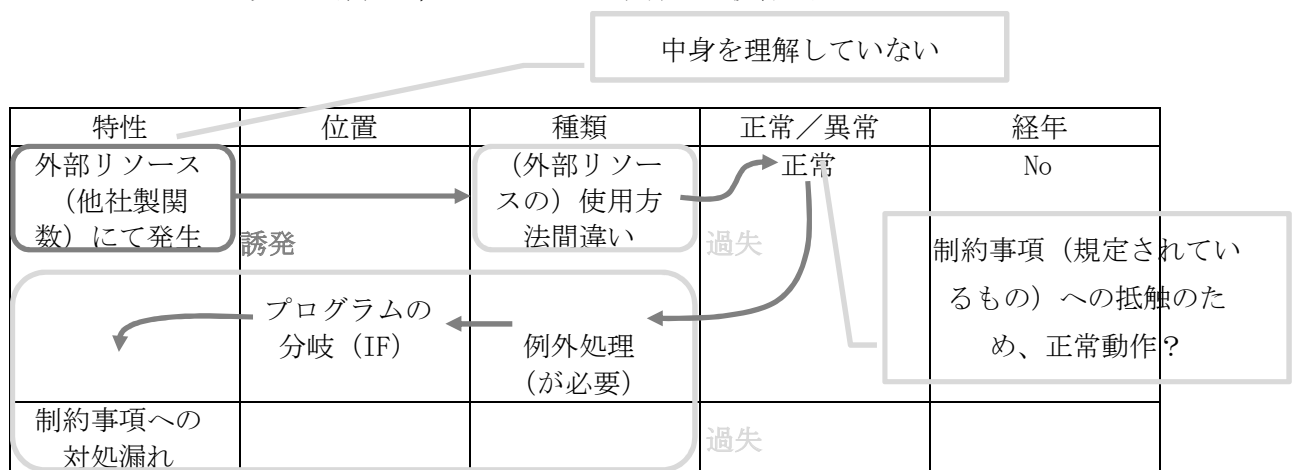
外部(関数)の動作チェック忘れ ※動作確認をしてから使っていなかった

誘発因子：外部(関数)利用までのプロセスが明確になっていなかった

※動作チェックや、制約事項の調査方法など

外部(関数)利用時に必要となるスキル(知識)の充足確認と教育不足

※充足を確認し、不足している場合には教育を実施



↓
バグ：他社製関数において、特定オブジェクトの位置の検知がされない

↓
結果：特定のオブジェクトの表示位置が出力されない

No. 3 : Objective-C で開発されたシステム

誘発因子	デバッグ環境なし	納期直前の仕様変更	簡単な修正	類似した長い変数名			
増幅因子	単体テスト未実施 目視による確認						
過失因子	変数名の酷似した別変数を参照？						
欠陥	手続区分の誤変換？						
表出現象	データ変更処理において手続区分 1 が 0 に勝手に変更される事象発生						

ソフトウェア欠陥の多属性表現 (MARS モデル)

故障モード：アクセスデータ読み込みの結果が異なる

種類：間違ったデータの取り込み

位置：データ生成処理部（条件文内での参照）

過失因子：誤った変数の使用

誘発因子：酷似した変数名

Type：ソフトウェア欠陥の多属性表現

特性	位置	種類	正常／異常	経年
・ IDE の利用 ・ 酷似した変数名を持つ変数多数	内部変数 誘発	変数の誤選択 過失	正常	No (仕様変更)
・ 異例処理がない	条件文 (IF) 誘発	必ず正常値を返す 過失	異常 誘発	Yes (既存ロジック)

↓
バグ：期待しないデータの取り込み × 必ず正常値を返す

↓
結果：期待された結果が出力されないことがある

No. 4：自社システムに取り込むため、受信ファイルのフォーマットチェックを行うバッチ

タグ	改善欲求	バイアス原因		縦割り組織	
		信頼実績	明記なし		
誘発因子	S/W 品質を改善したいという 開発者の欲求	過去に Null が原因の業務 トラブルなし	追加データは Null 無しが明記 されていたが、既存データにつ いては記載なし	業務システ ム開発は 別チーム	客先には相談 しづらい
過失因子	—	業務システムでは使用していないカラムがあることを知らず、 既存データも“全て Null を含まない”仕様であると認識			—
	既存バッチで Null チェックをしていなかったことは、 データフォーマットチェック漏れの潜在バグであると判断				—
	既存データに対する Null チェックの可否を客先に確認しなかった				
欠陥	HEX(0)を含む可能性のあるデータに対する Null 有無チェック				
増幅因子 (好欠乏性)	客先の受入テストでは、HEX(0)を含まないファイルのみ客先のシステムから送信				
表出現象	客先のシステムから送信された HEX(0)を含むファイルの取込処理にて、 不正なファイルを受信したとしてバッチが異常終了				

ソフトウェア欠陥の多属性表現 (MARS モデル)

故障モード：受信データの Null チェック適用誤り

対象・位置：受信データ

種類：Null チェック適用誤り

過失因子：①既存カラムに対する Null チェック実施

誘発因子：①受信データのカラム追加（仕様変更），②追加カラムは Null（終端文字）

無しの仕様，③追加カラムへの Null チェック実施 ④I/F 仕様書に既存カラムの Null 有無の記載なし

特性	位置	種類	正常／異常	経年
- 仕様追加 - HEX(0)を含む既存カラム - Null を含まない追加カラム	受信データ (I/F) 誘発 増幅	Null チェック適用誤り 過失	異常 誘発	Yes (既存)

バグ：受信データに対する Null チェック適用誤り

結果：終端文字でない HEX(0)を検出

No. 5：画面操作アプリケーション

誘発因子	2 度押しを防止する要求は明確であったが，マウス操作に対する実装方法が統一されていなかった。
増幅因子	マウス操作による業務処理が複雑である。業務ノウハウを理解している担当が少ない。
過失因子	機能実現に焦点が当たっており，実装方法の必要十分性を評価するという意識がなかった。
欠陥	ボタンの活性とボタンのチェックの両方を設定した。
表出現象	マウスで特定のボタンを押下するとボタン内の文字が表示ブレする

ソフトウェア欠陥の多属性表現（MARS モデル）

種類：過度の設計／追加実装によるイベント競合

正常／異常：異常系

位置：イベント取得処理（2 度押しによるイベント誤検出の防止）

特性：既存コードの改修。マウス操作が多く・複雑。2 度押しが回避できたため，実装方法に問題なしと思い込んだ。

経年・変化：既存コードを削除できない

特性	位置	種類	正常／異常	経年
増幅 既存コードの改修。マウス操作が多く・複雑。2 度押しが回避できたため，実装方法に問題なしと思い込んだ。 誘発	イベント取得	過度の設計 追加実装によるイベント競合	異常 過失	YES（既存コードを削除できない） 誘発

↓

バグ：ボタン操作に対し複数イベントの設定

↓

結果：イベントの重複による画面表示の乱れ

No. 6 : 画面操作アプリケーション

誘発因子	ウィンドウ操作イベントの理解不足，ウィンドウ操作イベントに対する注意点やノウハウ集の欠如
増幅因子	ウィンドウ操作による業務処理が複雑である。業務ノウハウを理解している担当が少ない。
過失因子	ウィンドウ操作イベントを取得できないタイミングがあることを意識していなかった。
欠陥	利用したウィンドウ操作イベントの誤使用
表出現象	ウィンドウ操作不可

ソフトウェア欠陥の多属性表現（MARS モデル）

種類：タイミングエラー（マウス操作イベントには，タイミングによりイベントを取得できないものがある）

正常／異常：異常系

位置：マウスの操作イベント

特性：異常処理に対する考慮もれ

経年・変化：No

特性	位置	種類	正常／異常	経年
異常処理に対する考慮もれ 過失	マウスの操作イベント	タイミングエラー 誘発	異常	No
知識不足（マウス操作イベントには，タイミングでイベントを取得できないものがある）				

↓ **増幅**

バグ：利用したウィンドウ操作イベントの誤使用

↓

結果：ウィンドウ操作不可

No. 7：受信処理不正

誘発因子	これまで不正データを受信したことがなく、従来ロジックで問題なかった。 これまで、大きなデータを受信したことがなく、従来ロジックで問題にならなかった。（WEB 関係のサービスの増加などで、他社の SW 変更量が増加し、その関係でデータの量が増加）
増幅因子	データ受信様式の変更のみの軽微な変更であった。 変更箇所について、要求仕様、設計、コードの追跡性を確保できていなかった。
過失因子	データ受信様式の変更であり、既存処理に大きな変更は必要ないと判断。移植時にデータ範囲を考慮せずに、範囲を狭めた。
欠陥	確保したバッファのサイズを超えてデータを書き込んだ為、バッファオーバーフローが発生。
表出現象	リブートを繰り返す

ソフトウェア欠陥の多属性表現（MARS モデル）

種類：齟齬，例外処理抜け，バッファオーバーフロー

正常／異常：異常系

位置：I／F

特性：一人では出せない。

経年・変化：Y E S（他社，新たなデータ様式）

特性	位置	種類	正常／異常	経年
① 一人では出せない	I/F	誘発 齟齬	異常系	Y E S (他社)
② 従来処理の継承 増幅		例外処理抜け 過失		誘発

↓
バグ：バッファオーバーフローでリセット

↓
結果：無現ループ

No. 8 : 初期化処理不備

誘発因子	従来の初期化処理が起動タイミングに依存する設計となっていた。従来設計時の異常状態の考慮漏れ。
増幅因子	通信サーバであり，システム停止状態時間を短縮することに多くの考慮が向いていた。
過失因子	タイマー処理の改修ではなく，別処理の改修に伴うシステム再立上げであった。従来，タイマー処理は問題なく実行されていたため，影響有無を確認しなかった。
欠陥	システム改修による通信サーバの停止によるデータ初期化処理の未実行。
表出現象	システム改修に伴い通信サーバを再起動した。その際に，タイマー処理によるデータ初期化処理が抜け，不正データを他装置に送付した。

ソフトウェア欠陥の多属性表現（MARS モデル）

種類：例外処理抜け

正常／異常：異常系

位置：起動タイミング

特性：24 時間運転が基本，当該処理自体の変更なし

経年・変化：Y E S（他機能の改修）

特性	位置	種類	正常／異常	経年
他機能改修による当該修理へのタイミング変化の考慮漏れ。当該処理自体の変更なし 誘発	起動 タイ ミン グ	例外処理抜け 過失	異常系	Y E S (他機能の改修) 誘発

↓
バグ：システム改修による通信サーバの停止によるデータ初期化処理の未実行

↓
結果：データ初期化処理が抜けにより，不正データを他装置に送付

以上