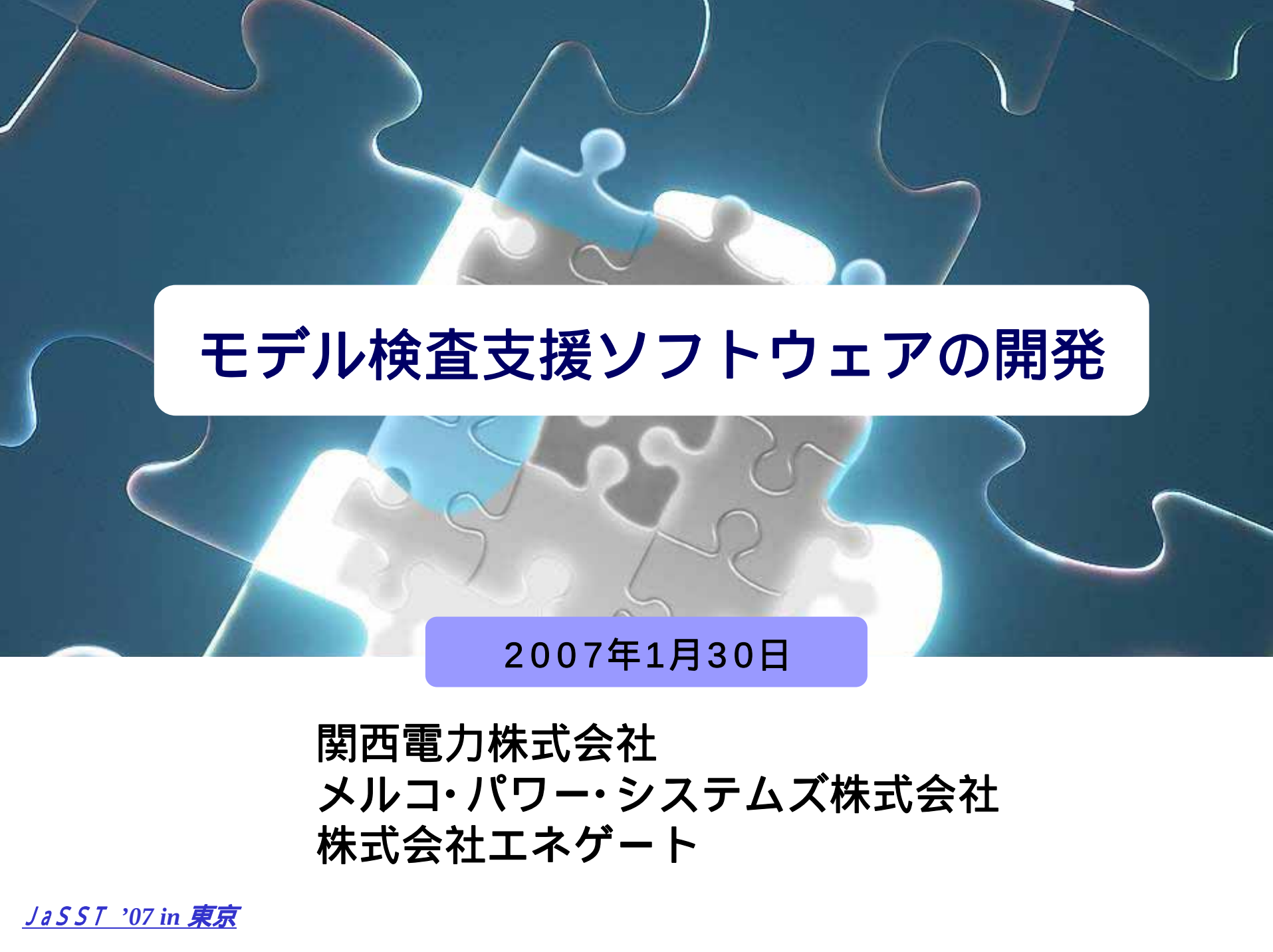




モデル検査支援ソフトウェアの開発

2007年1月30日

関西電力株式会社
メルコ・パワー・システムズ株式会社
株式会社エネゲート

はじめに

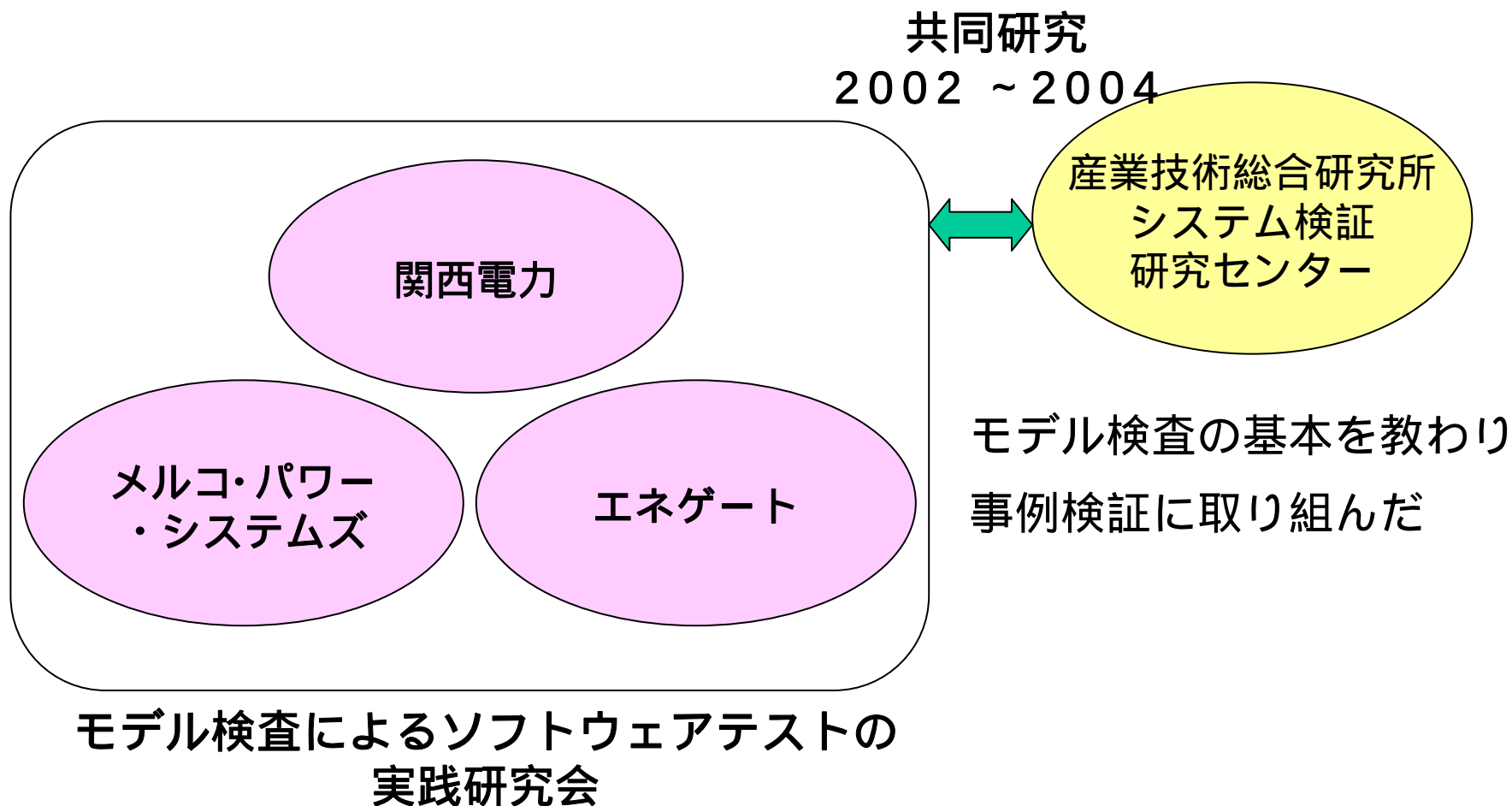
モデル検査の作業

作業支援の検討

モデル検査支援ソフトウェア

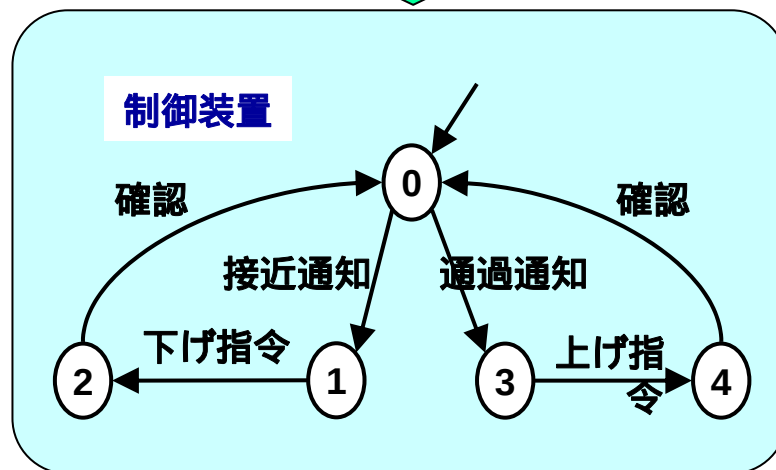
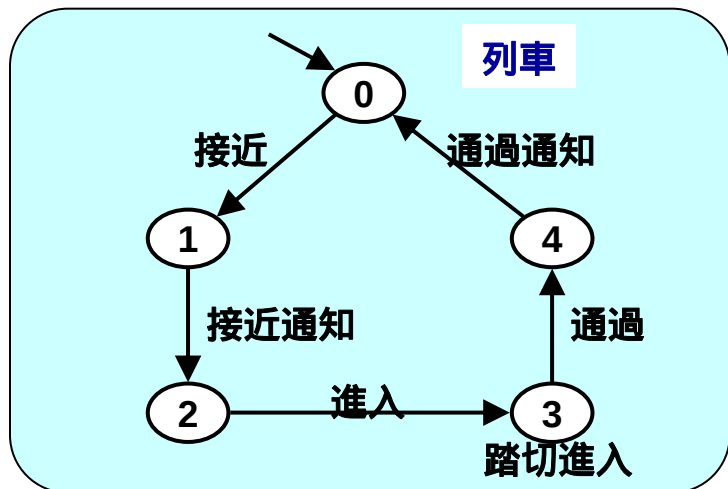
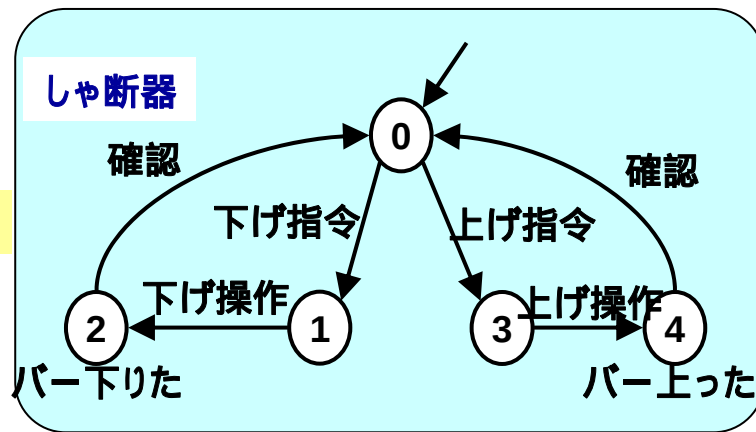
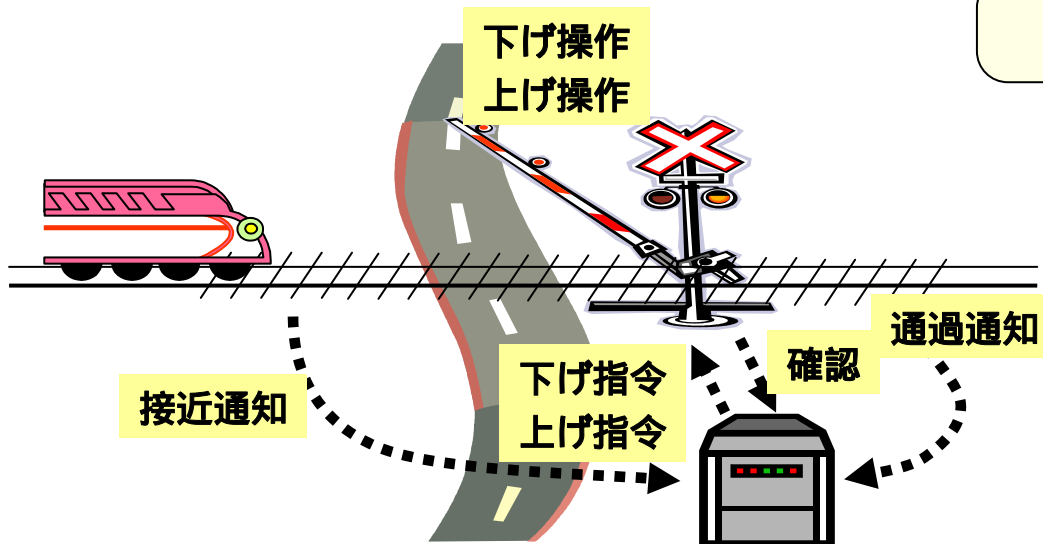
まとめ

背景



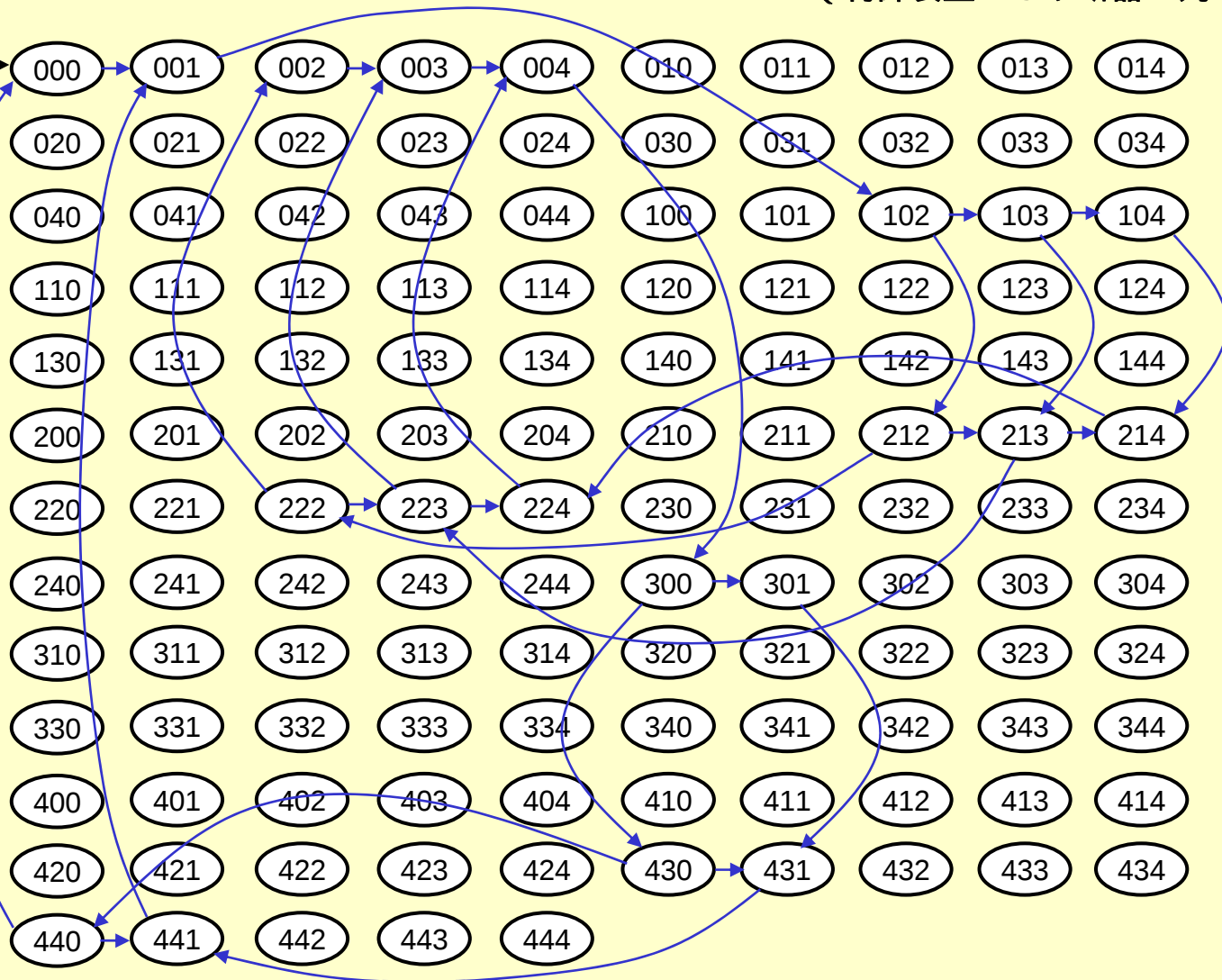
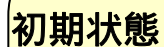
モデル検査の考え方

サブシステムの振舞いをモデル化



システム全体の状態と状態遷移

(制御装置：しゃ断器：列車)

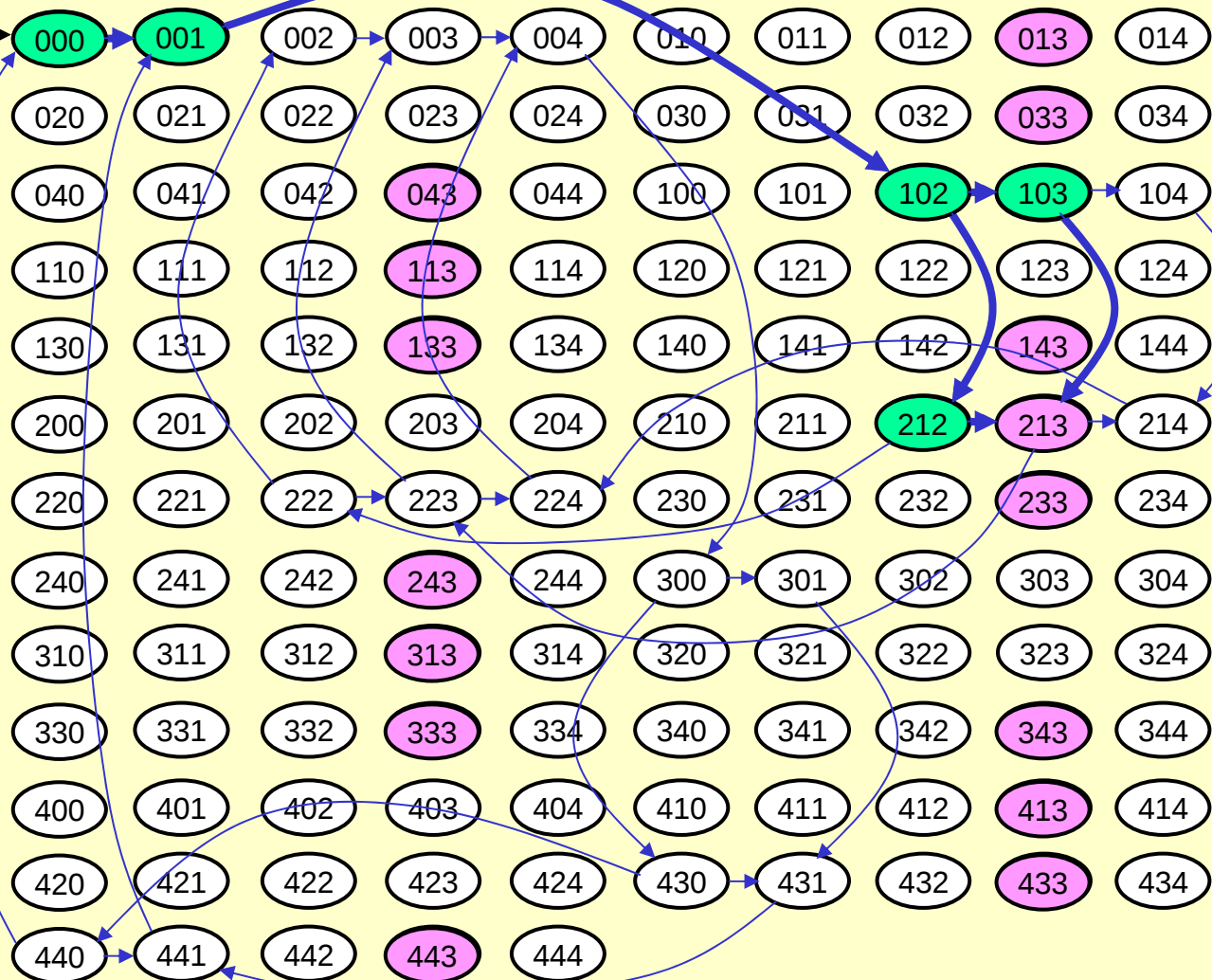


初期状態から検査したい状態へ到達できるか

初期状態

状態集合 F_T の
前状態集合 F_{T-1}
に初期状態が
含まれていれば
システムは、
起動後に不具合
事象に到達する
場合がある

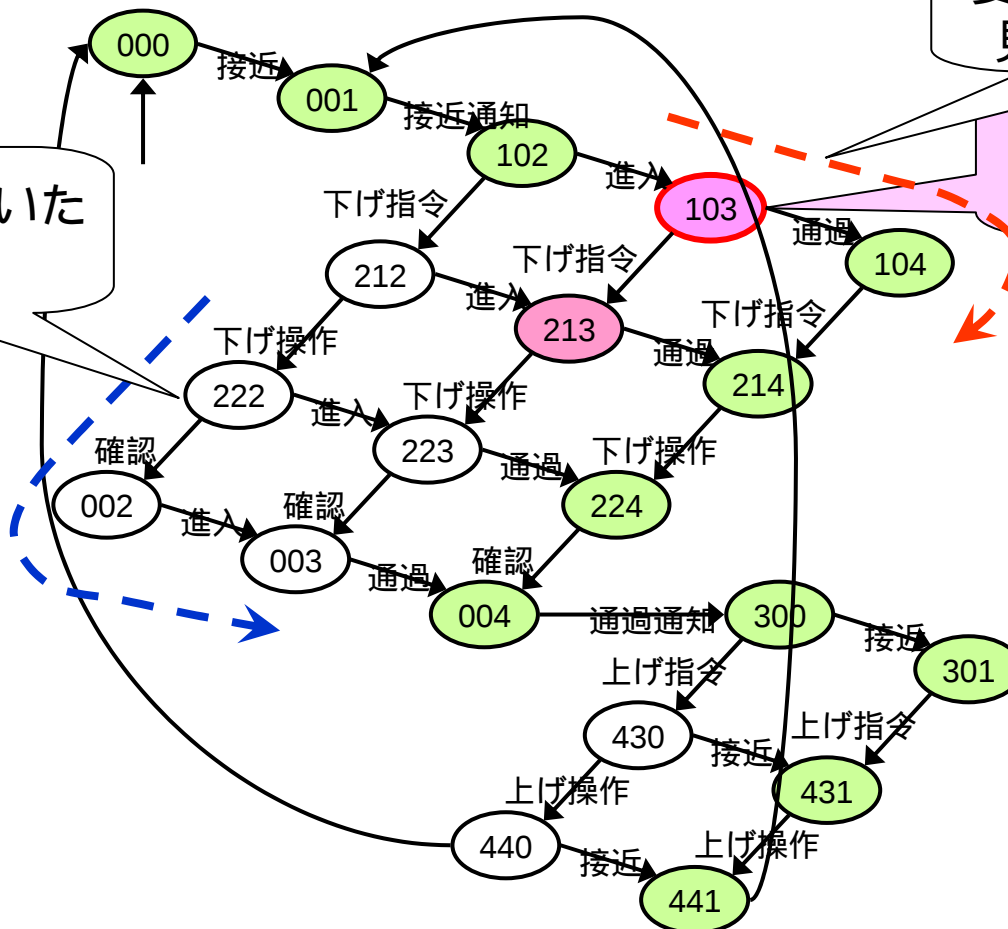
論理的な操作
手順により、
不具合事象発
生の可能性を
確実に検出
できる。



モデル検査の反例

反例出力される状態遷移図

設計者が考えていた
安全な経路



要素モデルの組合せで
見つかる危険な経路

しゃ断器バーが下
りる前に列車進入



モデル検査のポイント

1. 検査したい要素がモデルに書かれていること
(状態にないものは検査できない)
2. システムの部分モデルを作れば良い
(全体モデルは自動生成される)
3. テストデータは不要
(データや外部入力もモデル化して扱う)
4. 検査の目的によってモデルが違う



はじめに

モデル検査の作業

作業支援の検討

モデル検査支援ソフトウェア

まとめ

モデル検査の作業の流れ

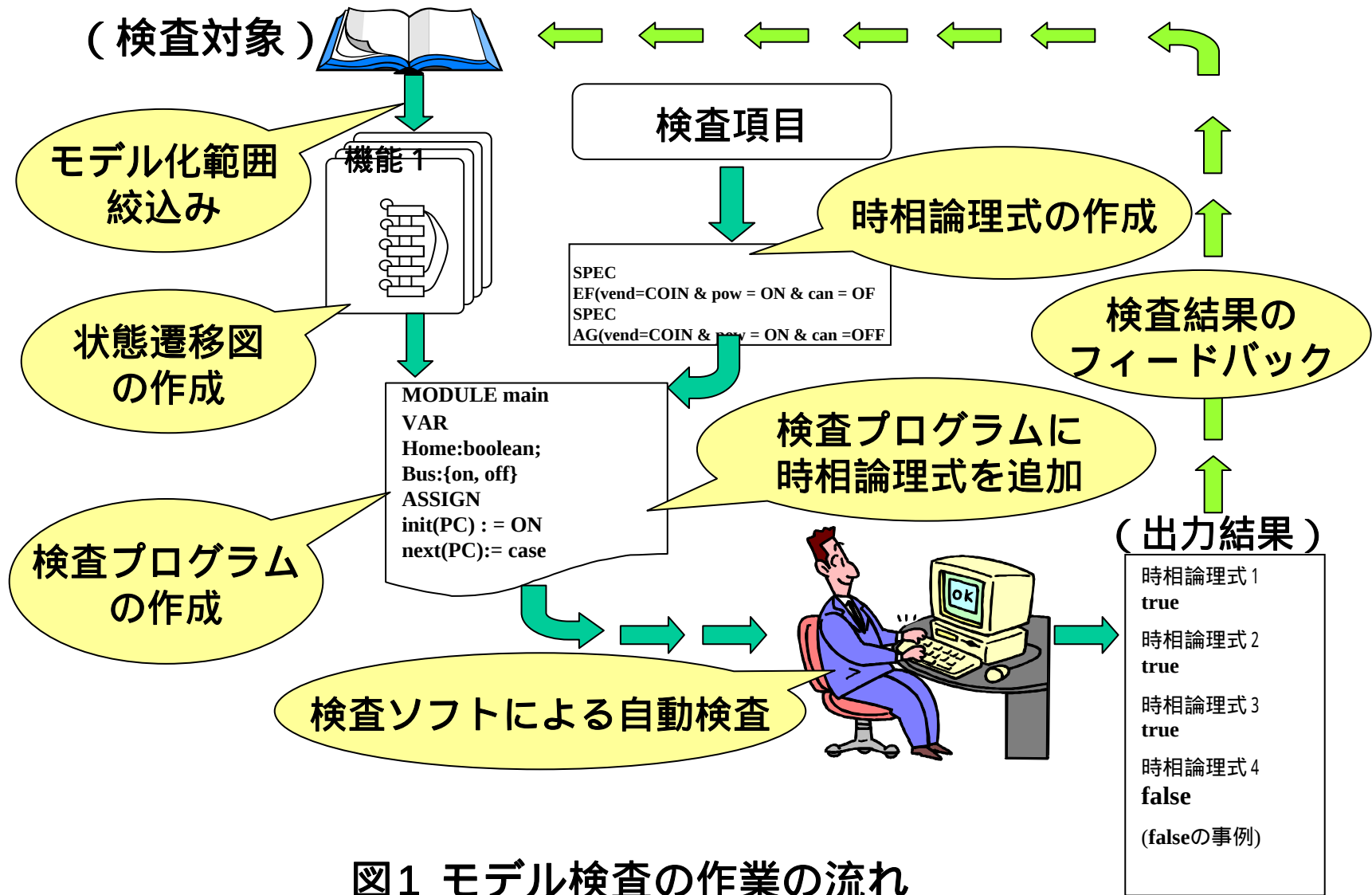
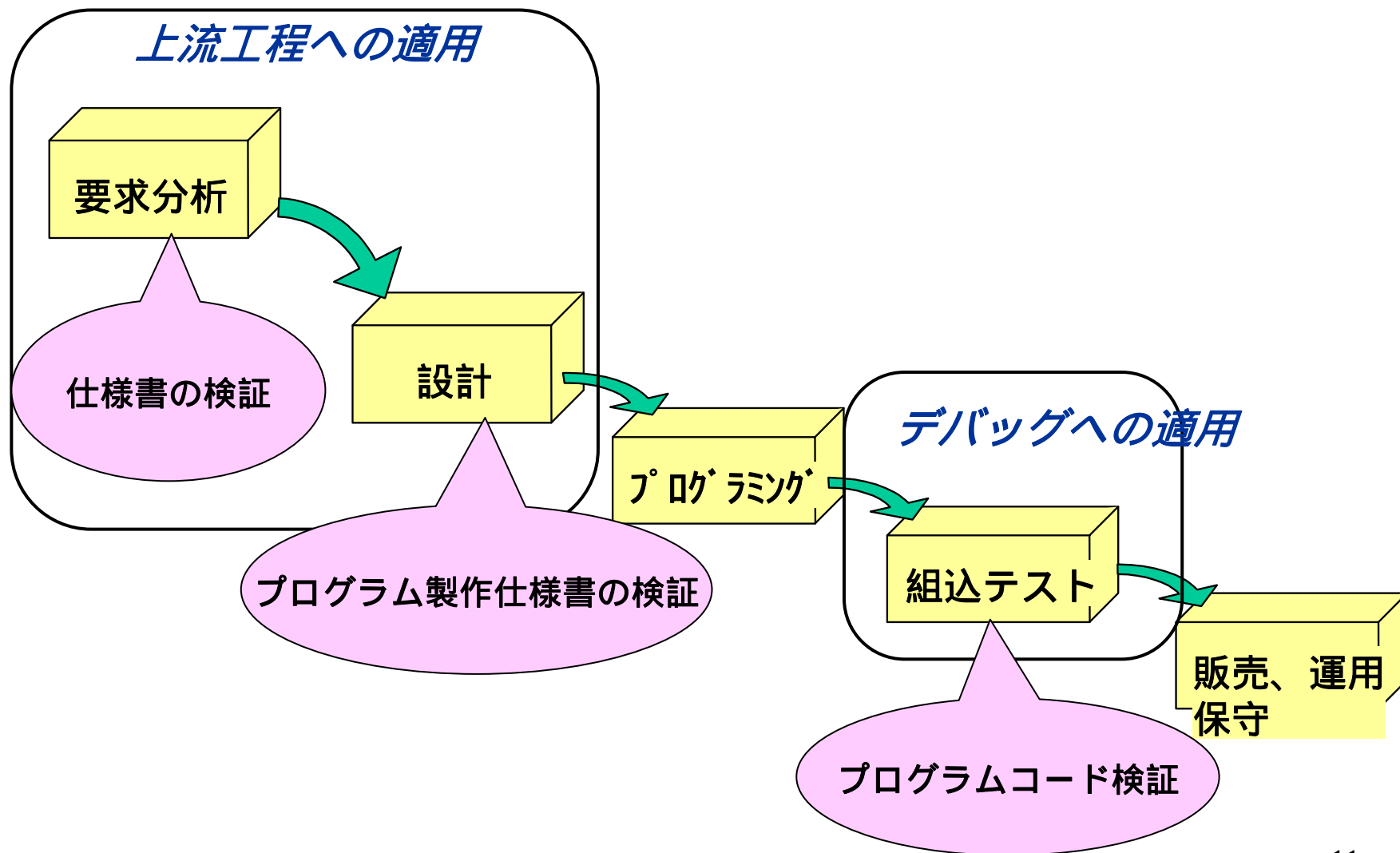


図1 モデル検査の作業の流れ

ソフトウェア開発工程での適用



モデル検査適用の経験

組み込みソフトウェア

監視制御ソフトウェア

	仕様書の検証	設計仕様書の検証 (～160H、7件)	コードのデバッグ (～50H、3件)
検査項目	要求仕様どおりに データ書替 デッドロックしない	外部入力の変動に 追従して切替できるか	稀にデータ取得せず テスト時に一度だけ 不正出力
発見したバグ	想定外の書替手順 タイムアウト記述忘れ	想定外の変数アクセス 想定外の割り込み 想定外の外部入力 割り込みのオーバーヘッド	ループ文の誤り コメントアウトの誤り



はじめに

モデル検査の作業

作業支援の検討

モデル検査支援ソフトウェア

まとめ

モデル検査の難しさ

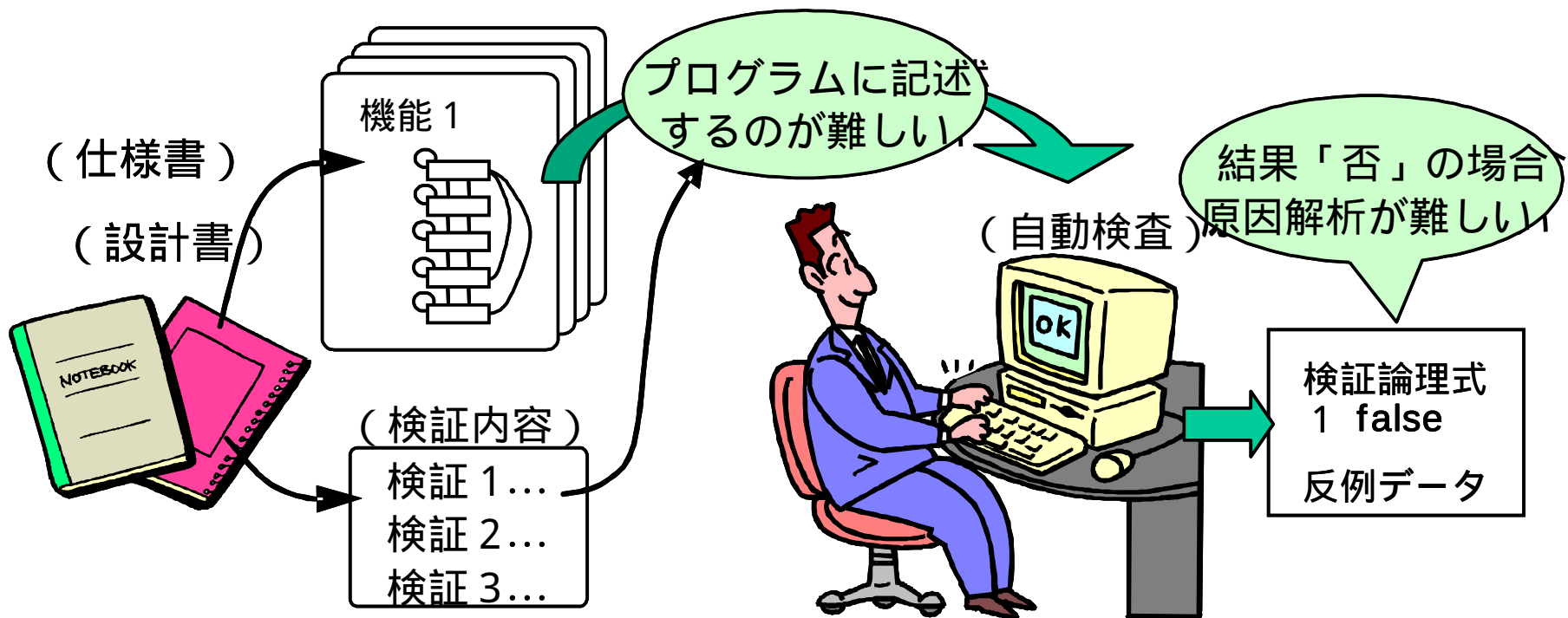
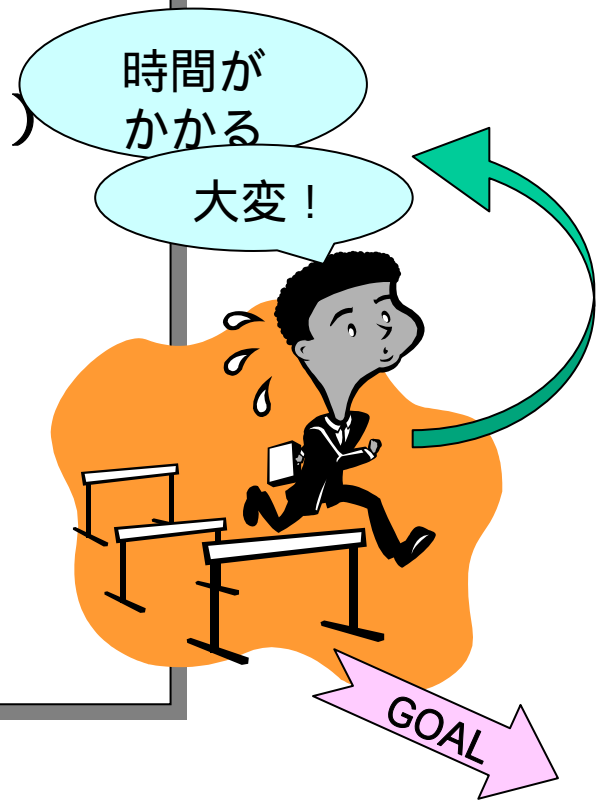


図2 モデル検査特有の作業の難しさ

モデル検査特有の作業

1. 検査プログラムの作成（モデル記述）
2. 検査項目の設定
3. 検査項目の記述（時相論理式）
4. 反例解析の手間



検査プログラムの作成

課 題

```
MODULE main
VAR
  CONTROLLER : 0..4 ;
  GATE : 0..4 ;
  TRAIN : 0..4 ;
  aux : boolean ;
```

難解なモデル記述

```
cmdnd_down := CONTROLLER=1 & GATE=0 & !aux ;
```

```
ASSIGN
  init(CONTROLLER) := 0 ;
  next(CONTROLLER) := case
    ind_near: 1;
    ind_out : 3;
```

対 策

モデル検査支援ソフトウェア

(図形入力からのモデル作成)

```
cmdnd_down: 1;
cmdnd_up: 3;
```



検査項目の設定

課 題

新規システムに対する
検査項目の決定



対 策

仕様書に基づく

別の種類のドキュメント
対象システム分野の知識
業界の常識

検査項目の記述

課題

$AG(P)$ $EG(P)$
 $AX(P)$ $EX(P)$
 $AF(P)$ $EF(P)$
 $A[P \cup Q]$ $E[P \cup Q]$

CTL?

時相論理式による記述

対策

良く使うパターンを支援ソフトウェア
に収録

(モデル中に補助パラメータを追加)

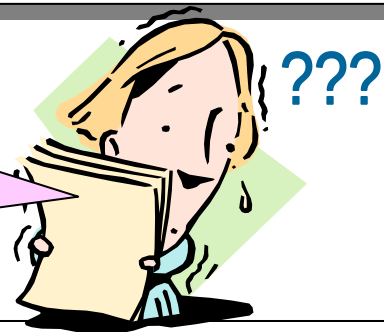
反例解析の手間

課題

反例に示された不具合内容の読取

対策

ステップ毎に
全変数の値が
出力される



検査項目に関する変数の抽出と
並べ替え
フロー図、状態遷移図への遷移関係の
表示

はじめに

モデル検査の作業

作業支援の検討

モデル検査支援ソフトウェア

まとめ

モデル検査支援ソフトウェアの構成

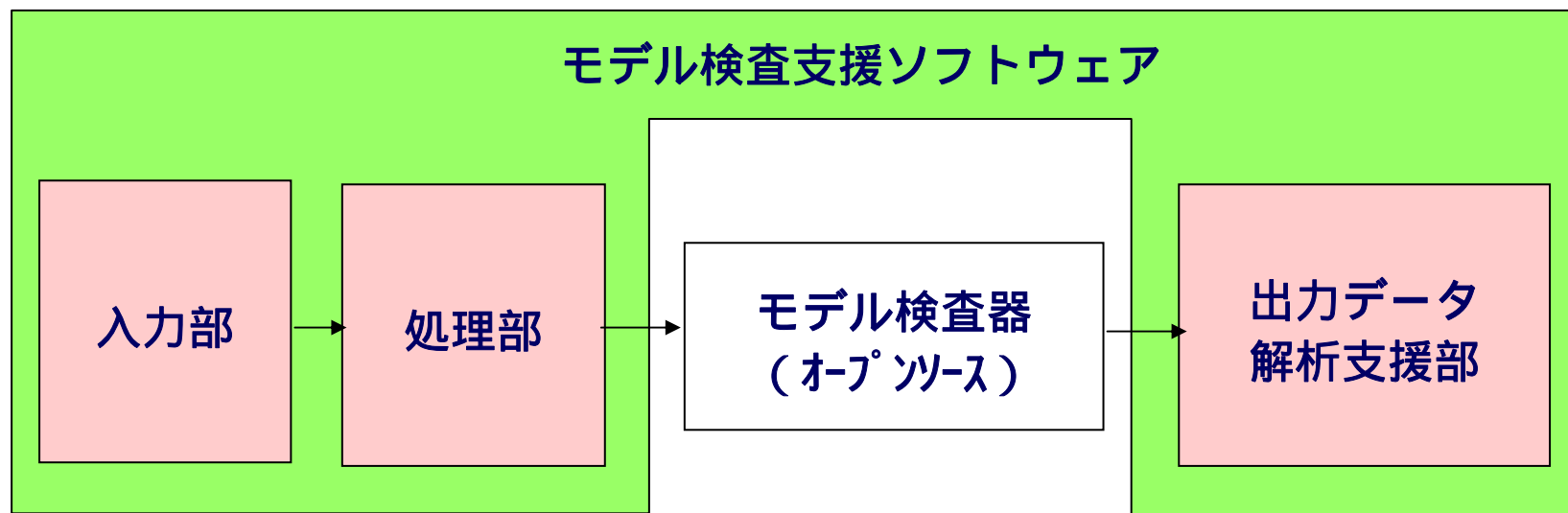
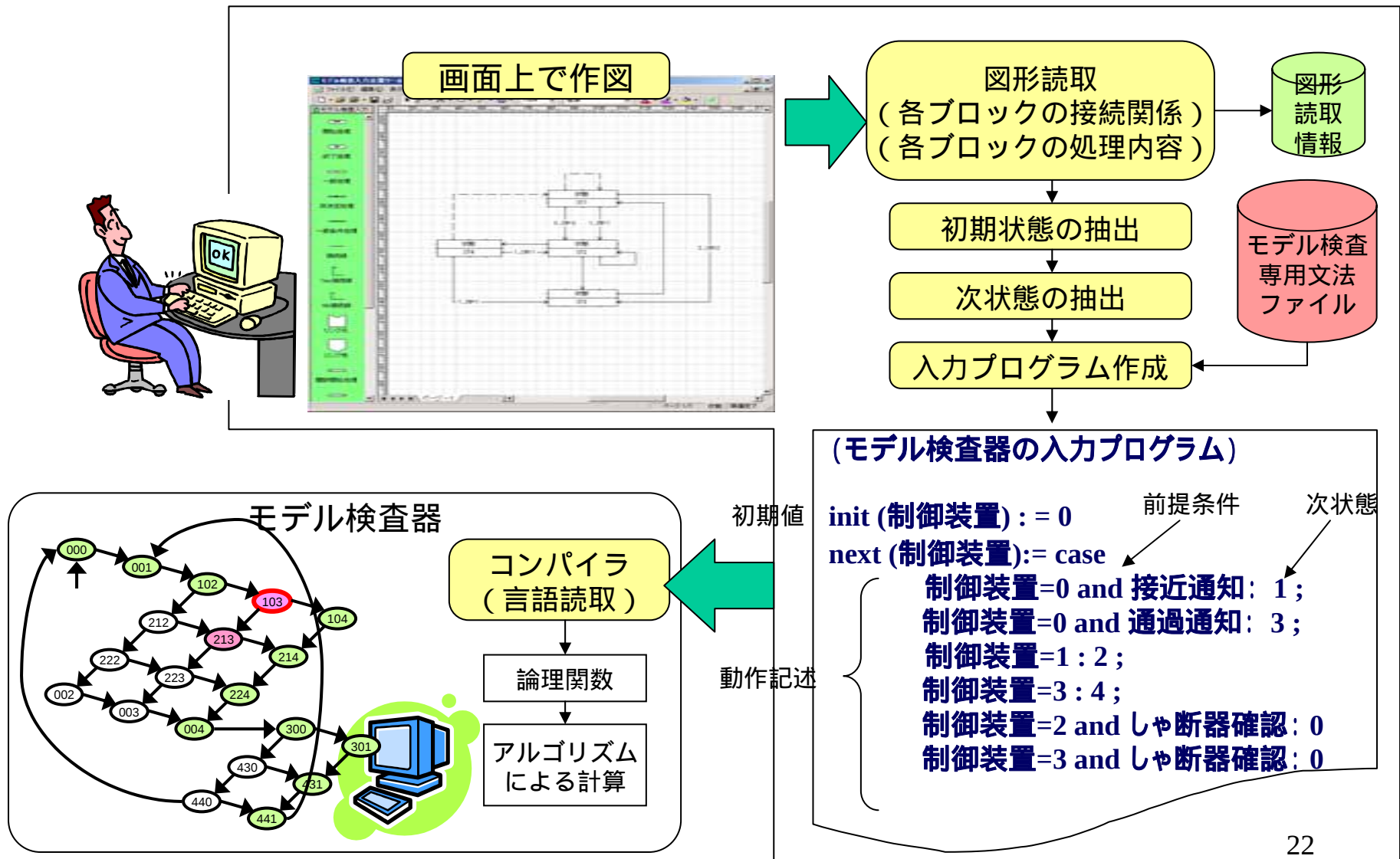


図4 モデル検査支援ソフトウェアの構成

モデル検査支援ソフトウェアによるモデル作成



モデル検査支援ソフトウェアによる反例解析

モデル検査器

モデル検査実施

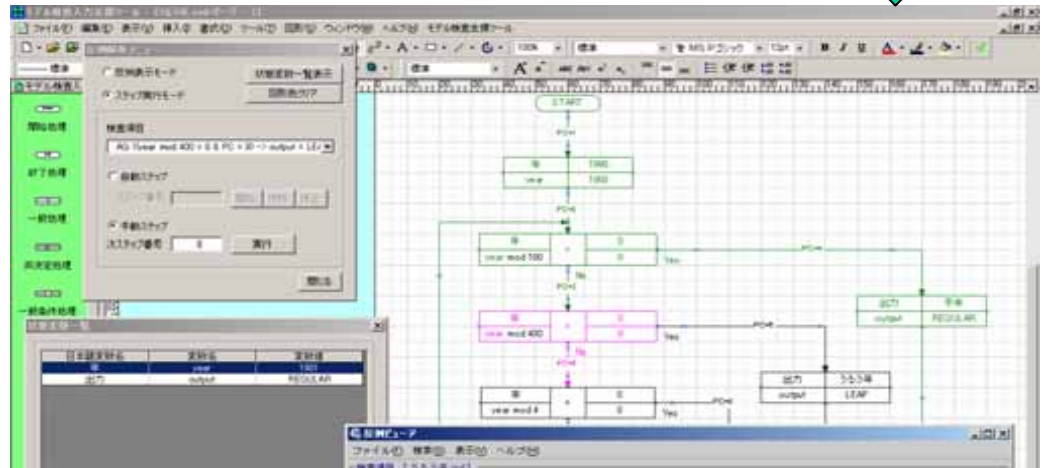
反例データ
出力

反例ビューアの作成

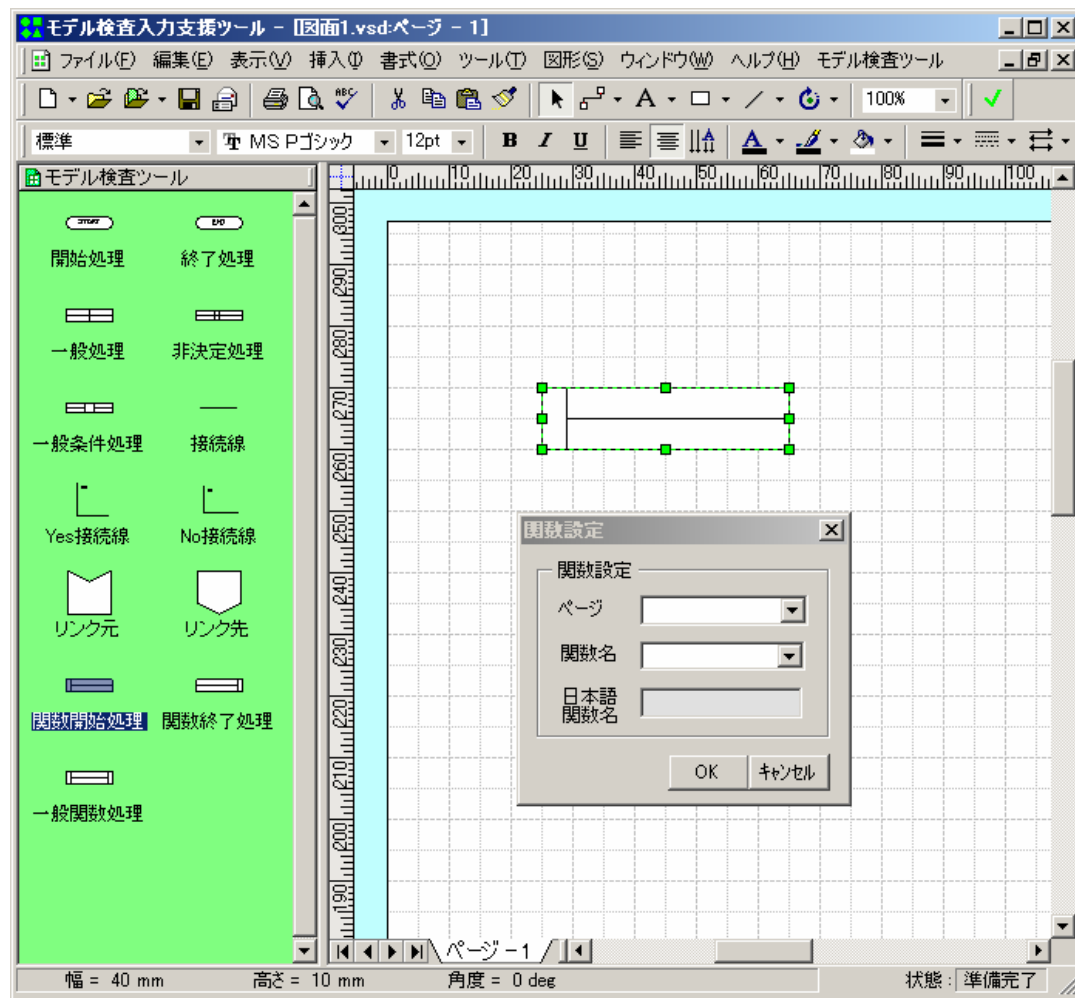
	1	2	3	4	5	6	7	8	9	10	11	12
PC_MAH	0	1	2	4	5	5	5	5	5	5	5	5
PC_TSS	0	0	0	0	0	0	0	0	0	0	0	0
PC_TSSn	0	0	0	0	0	0	0	0	0	0	0	0
PC_TSSn	0	0	0	0	0	0	0	0	0	0	0	0
Enablest	NO	NO	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
SuicConform_Fig	End	End	End	End	End	End	End	End	End	End	End	End
SuicCPU_Wt	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT
SuicPower_Wt	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden
Power_Wt	22	21	20	22	21	19	18	17	16	15	14	
LastPower_On	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden	Tenden
MACTACT_OK	1	1	1	1	1	1	1	1	1	1	1	1
Power_Wt	L	L	L	L	L	L	L	L	L	L	L	L
Power_Wt	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Power_Wt	OFF	ON	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
Power_Wt	L	L	L	L	L	L	L	L	L	L	L	L
Power_Wt	L	L	L	L	L	L	L	L	L	L	L	L

フロー図情報による
図形との対応づけ

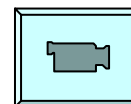
ステップ実行
(色変表示)制御



フローチャート・状態遷移図の作成



フローチャート



状態遷移図

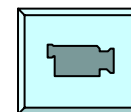


図5 モデル検査支援ソフトウェアの入力画面

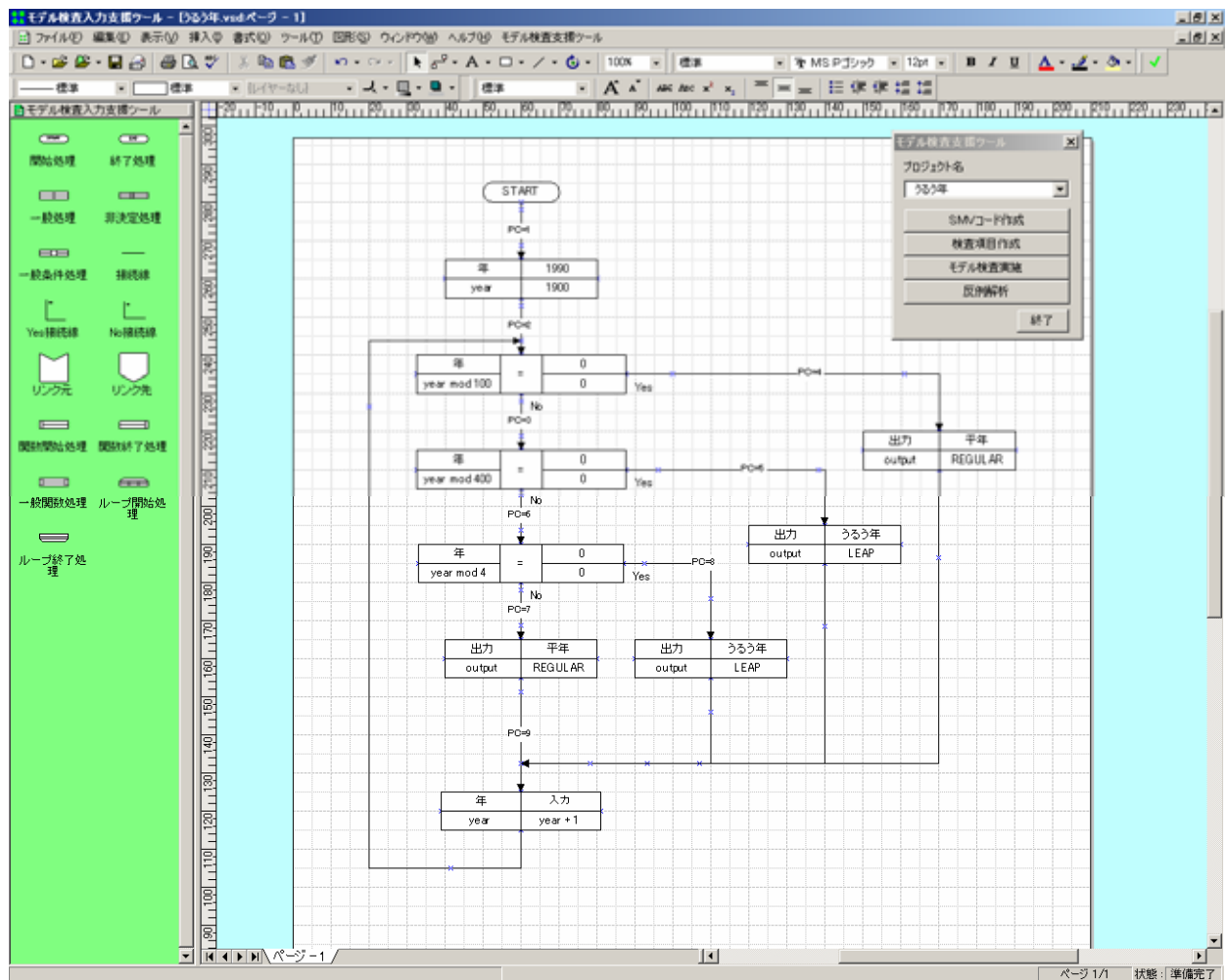


図7 モデル検査支援ソフトウェアを用いて作成したフロー図

検査プログラムの自動生成

```
MODULE main
  VAR
    year : 1900..2050;
    PC : 1..9;
    output : {LEAP, REGULAR};
  ASSIGN
    init(year) := 1900;
    next(year) :=
      case
        PC = 1 : 1900;
        PC = 9 : {1900..2050};
        1 : year;
      esac;
    init(PC) := 1;
    next(PC) :=
      case
        PC = 1 : 2;
        PC = 2 & year mod 100 = 0 : 4;
        PC = 2 & !(year mod 100 = 0) : 3;
        PC = 3 & year mod 400 = 0 : 5;
        PC = 3 & !(year mod 400 = 0) : 6;
        PC = 4 : 9;
        PC = 5 : 9;
        PC = 6 & year mod 4 = 0 : 8;
        PC = 6 & !(year mod 4 = 0) : 7;
        PC = 7 : 9;
        PC = 8 : 9;
        PC = 9 : 2;
        1 : PC;
```

自動生成された
検査項目

```
SPEC EF(year = 2050)
SPEC EF(PC = 1)
SPEC EF(PC = 2)
SPEC EF(PC = 3)
SPEC EF(PC = 4)
SPEC EF(PC = 5)
SPEC EF(PC = 6)
SPEC EF(PC = 7)
SPEC EF(PC = 8)
SPEC EF(PC = 9)
```

図8 フロー図から自動作成されたモデルと時相論理式

検査項目の記述

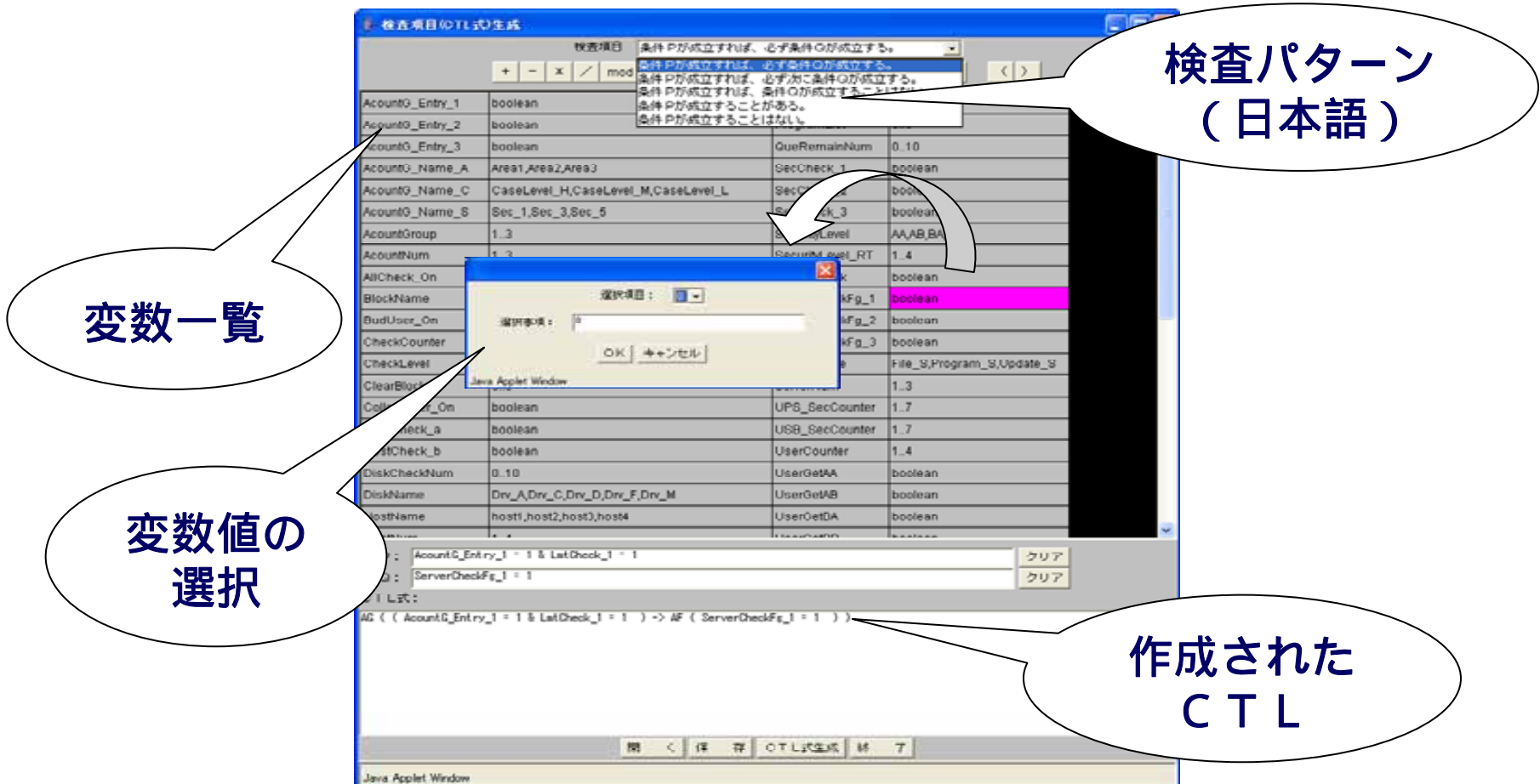


図9 検査項目の入力画面

モデル検査の実行

反例ビューア

ファイル(F) 表示(V) ヘルプ(H)

検証項目 [BaseUnitOut]

AG (((g_ucPower_Sts=Tuuden)&(Kensa_Time=22)) -> (AF ((Kensa_Time=0)&(is false

変数一覧 (ソート可)

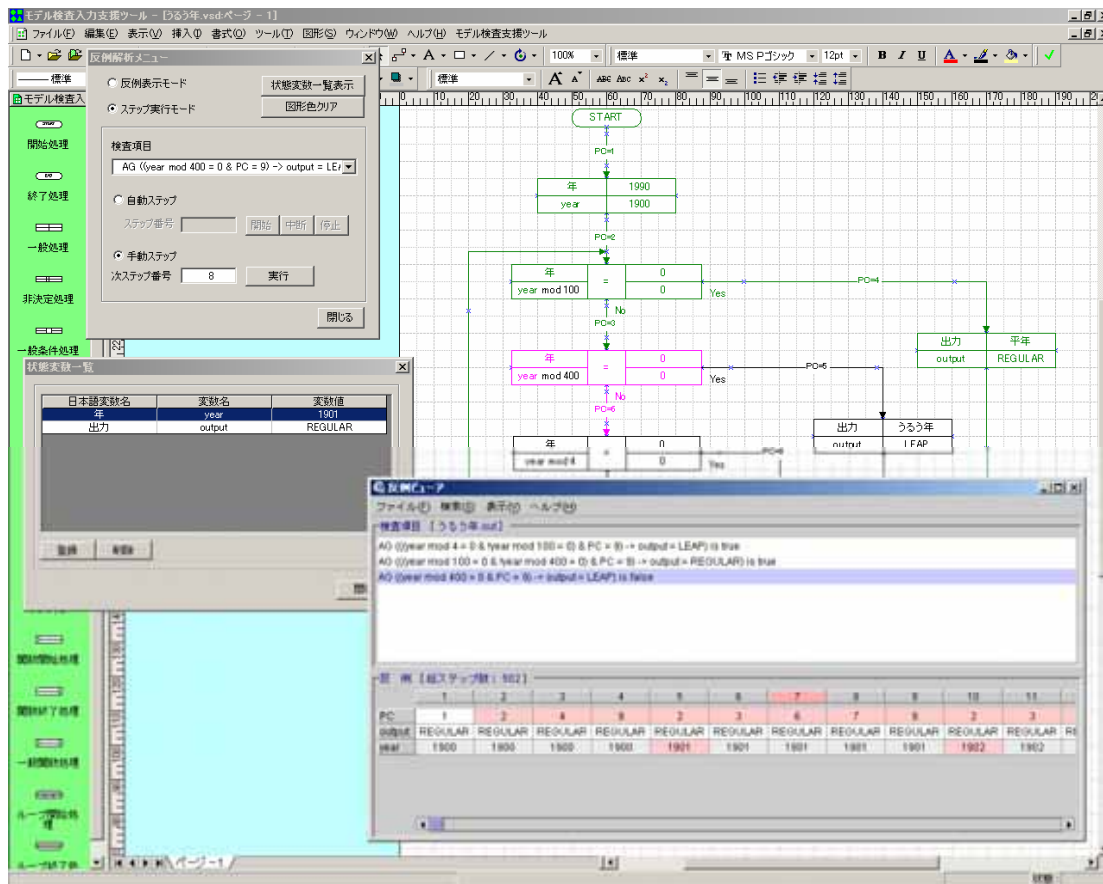
ステップ番号

ステップ数: 140 (ループ開始: 90)]

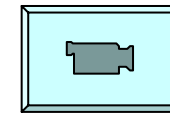
	1	2	3	4	5	6	7	8	9	10	11	12
C_MAIN	0	1	2	4	5	5	5	5	3	1	2	4
PC_T500	0	0	0	0	0	0	0	0	0	0	0	0
PC_Teiden	0	0	0	0	0	0	0	0	0	0	0	0
PC_Tuuden	0	0	0	0	1	2	3	0	0	0	0	0
EnableInt	NG	NG	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
g_ucCommBusy	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
g_ucConfirm_Flg	End	End	End	End	End	End	Kakunin	Kakunin	Kakunin	Kakunin	Kakunin	Kakunin
g_ucCPU_Sts	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT	WAIT
g_ucPower_Sts	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden
Kensa_Time	22	21	20	22	21	20	19	18	17	16	15	14
Last_Power_Sts	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden	Teiden
MAIN_ACT_OK	1	1	1	0	0	0	0	1	1	1	1	1
Powclk_Irpt	L	L	L	H	L	L	L	L	L	L	L	L
Powclk_Sts	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Power	OFF	ON	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
PowerEdge	L	L	H	H	L	L	L	L	L	L	L	L
PowerEdge Last	L	L	L	H	H	L	L	L	L	L	L	L

図10 モデル検査支援ソフトウェアの検査結果画面

反例の解析



変数の抽出



変数並び替え

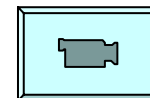
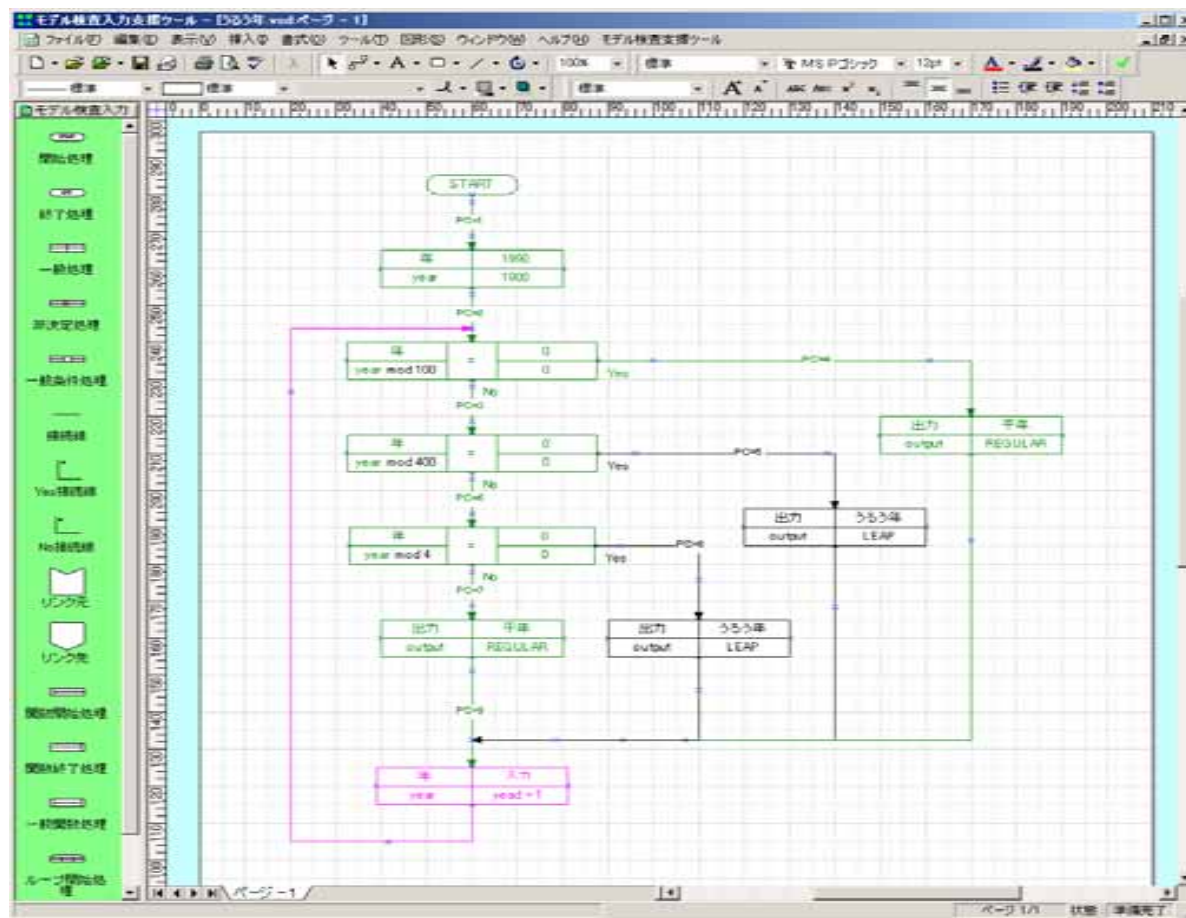
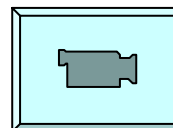


図11 モデル検査支援ソフトウェアを用いた反例解析画面

反例の解析 2



自動ステップ



手動ステップ

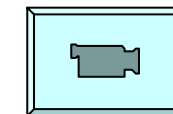
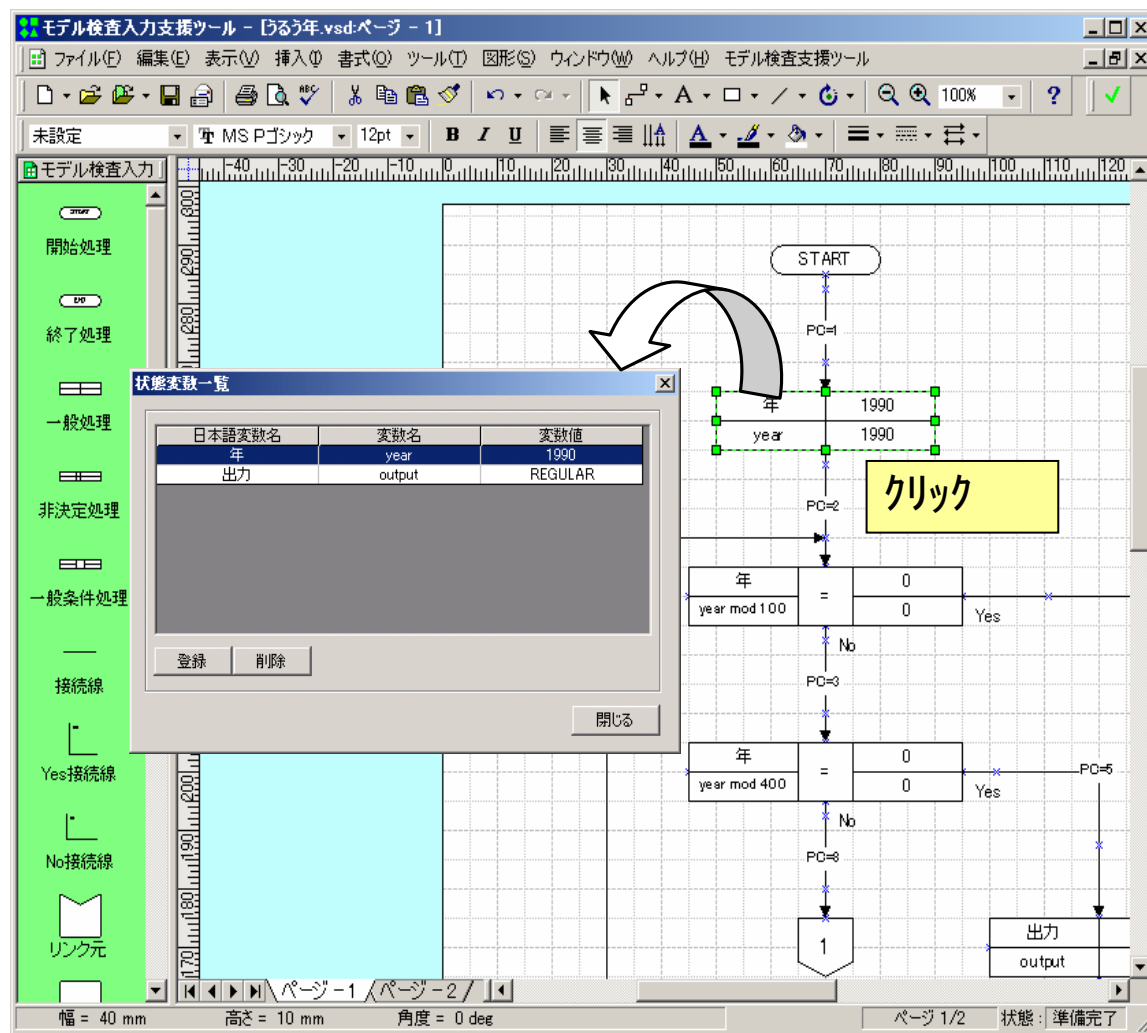
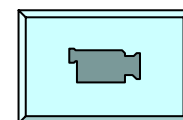


図12 反例によるフロー図の色替表示

反例の解析 3



変数値の表示



状態確認する変数の登録

モデル検査支援ソフトウェアの入出力機能

表 1 SMVと支援ソフトウェアの比較

		モデル検査器 S M V	モデル検査 支援ソフトウェア
入力	フロー図	×	○
	状態遷移図	×	○
	専用言語	○	○
出力	データ列	○	○
	チャート	(*1)	○
	フロー図反映	×	○
	状態遷移図反映	×	○

(*1) : モデル検査器により対応 / 非対応あり

効 果

- 1.モデル検査器を意識せずに対象システムの不具合解析に専念できる
- 2.モデル検査の基本を学習する必要性は不変
- 3.プログラム言語を使わない人も検査できる
- 4.作業が時間が短縮できる

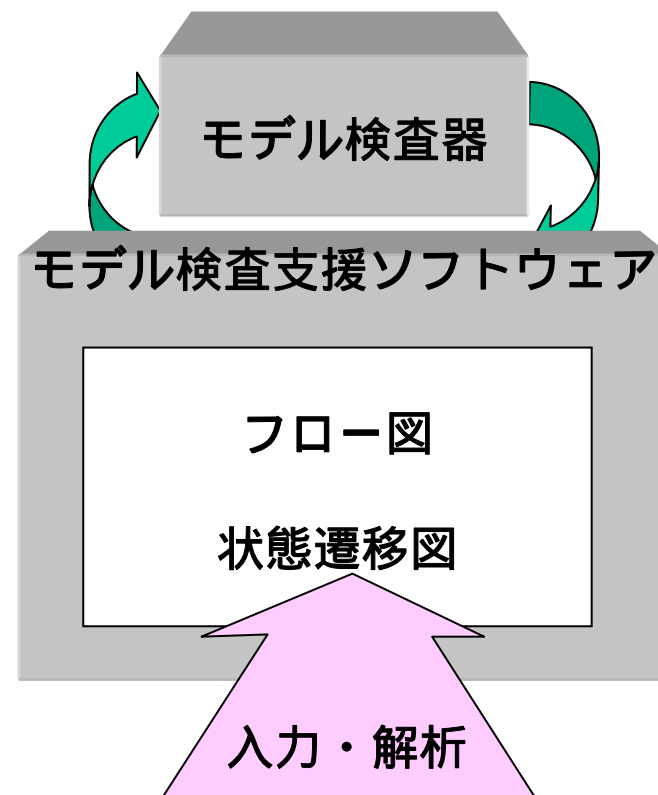


図13 モデル検査支援ソフトウェアの効果

モデル検査支援ソフトウェアによる作業支援



(試供版) をWebページから提供





ご清聴ありがとうございました

関西電力株式会社
メルコ・パワー・システムズ株式会社
株式会社エネゲート