高レジリエンス・システムのモデル化による検証例

形式手法の適用

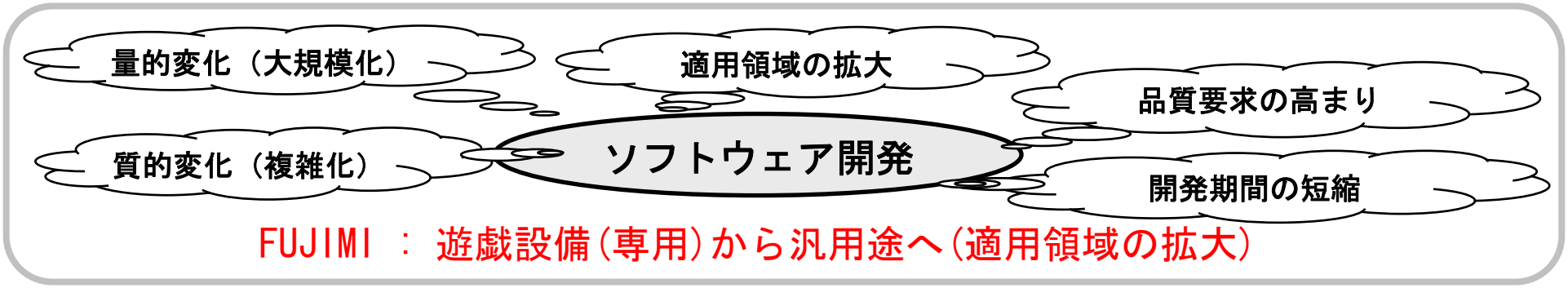
産業技術総合研究所
セキュアシステム研究部門　システムライフサイクル研究グループ

早水 公二　山形 頼之　林 伸行　大崎 人士

3. 形式手法の適用

3.1 技術背景

ソフトウェア開発を取り巻く環境



これまでは

職人技的な開発手法

一部の優秀な技術者の
技量や経験に頼る

パラダイム
シフト

これからは

工学的開発手法

開発／検査技術・管理技術
プロセス体系化

上流工程で数理的検証手法を適用して品質の確保・開発コストの削減等の課題を解決する。

形式手法(モデル検査)の適用

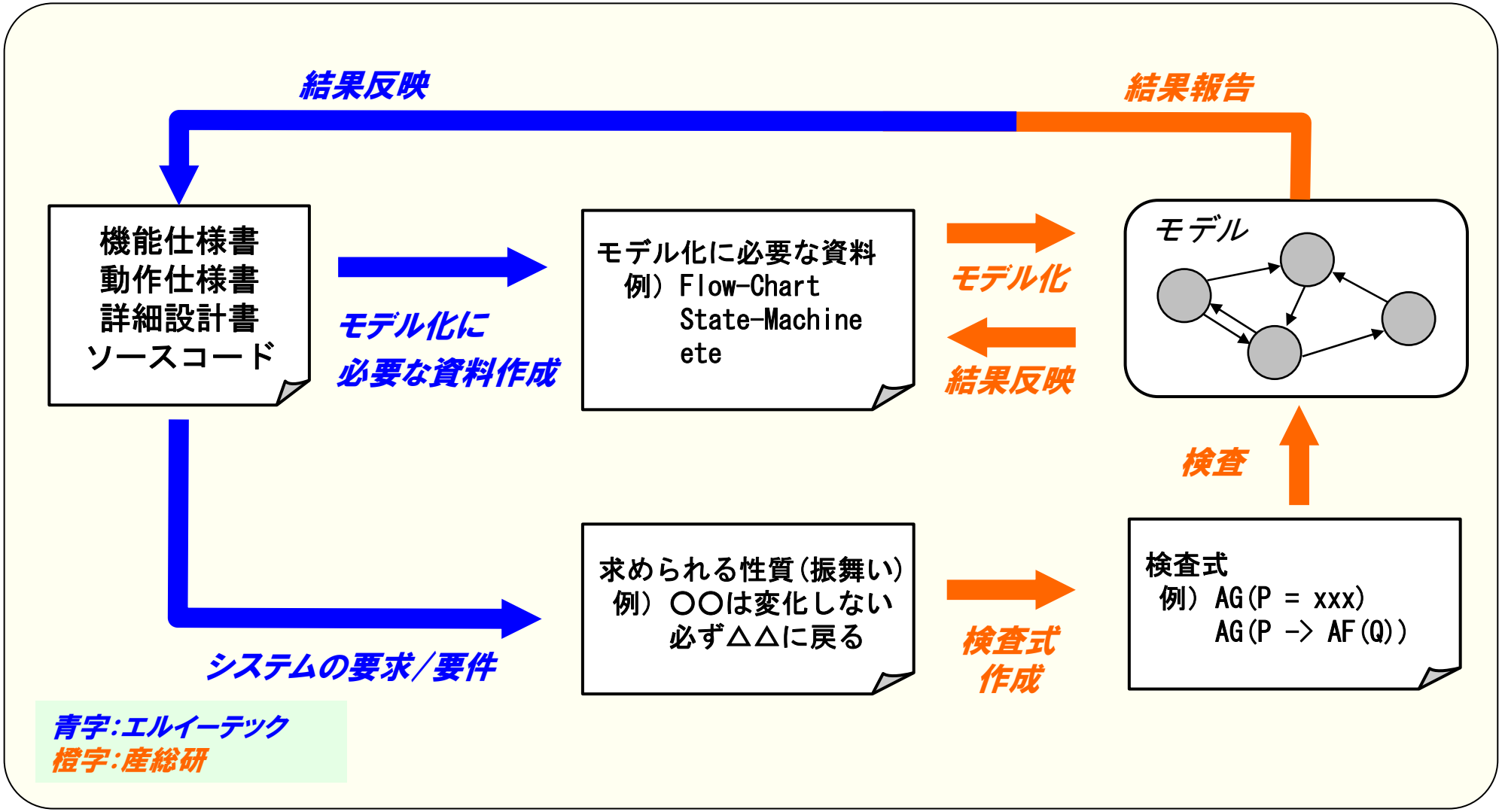
モデル検査ツール：SMV(Symbolic Model Verifier)

LETech

National Institute of Advanced Industrial Science and Technology
AIST
独立行政法人
産業技術総合研究所

3. 形式手法の適用

3.2 適用の流れと役割分担

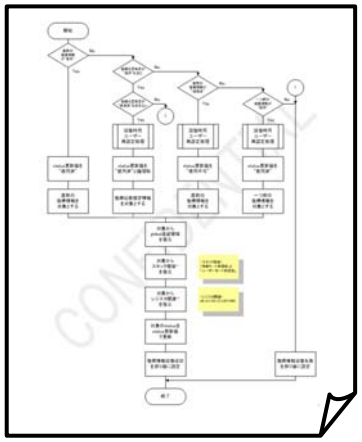


3. 形式手法の適用

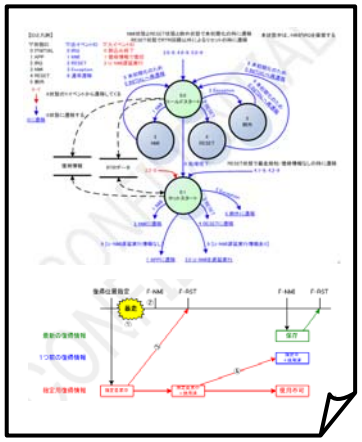
3.3 モデル化の進め方

状態爆発 ： モデルの状態が大き過ぎてメモリ不足が発生したり、
現実的な時間で検査結果が得られ無くなること

モデル化に必要な資料



Flow-Chart



State-Machine
Timing-Chart

モデル化

最大モデル

抽象化①

抽象化②

重要な要素（割込位置・頻度等）は維持

モデル①

■絞込みと抽象化無し

詳細モデル → 抽象モデル → 最適モデルへ
絞り込んでいく手法を採用

爆発

モデル②

■割込の抽象化

種類（低Level割込etc）の絞込みと
発生タイマ値の抽象化を実施

爆発

モデル③

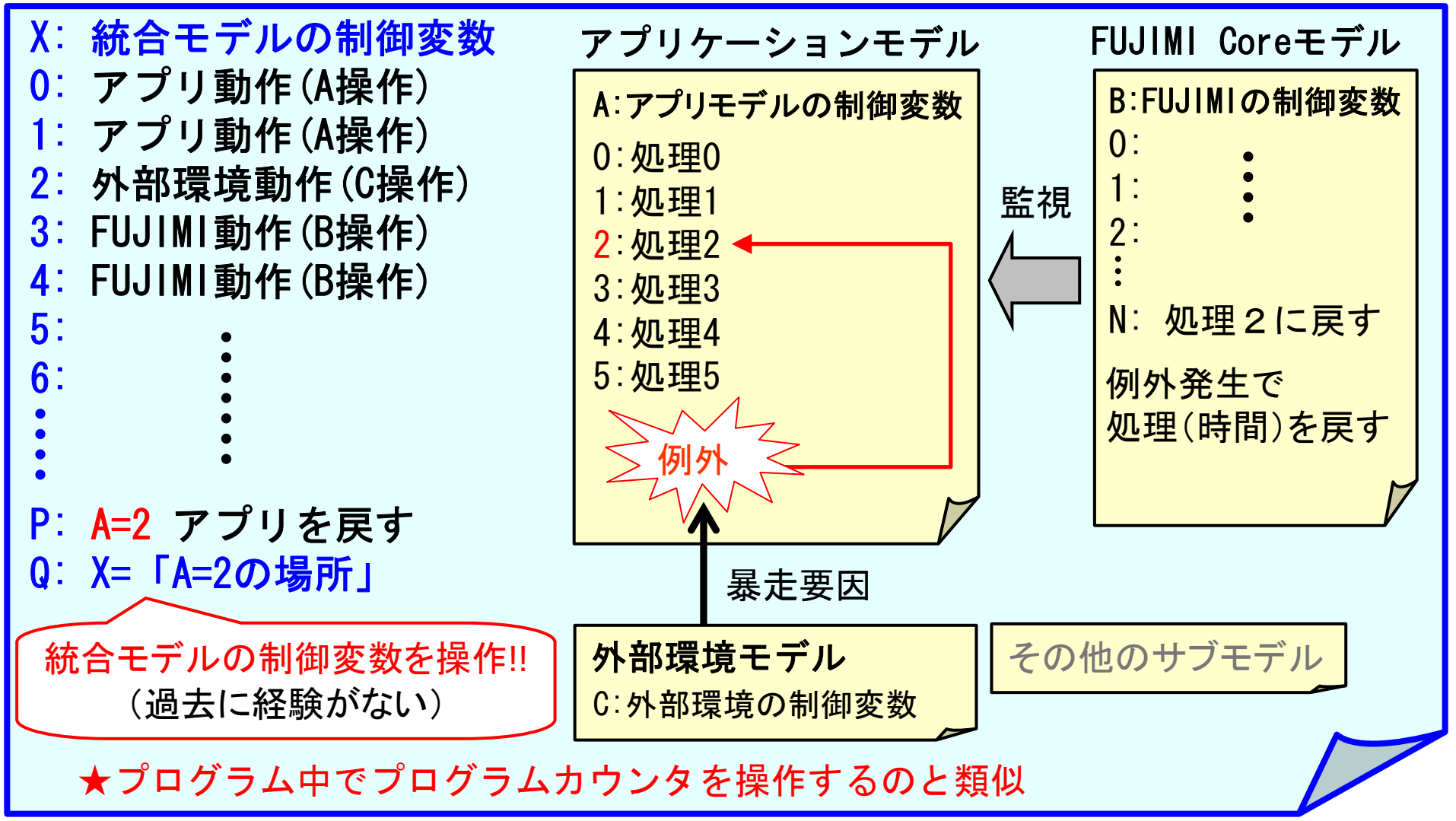
■CPU状態の抽象化

CPU状態の削減

OK

3. 形式手法の適用

3.4 モデルの特徴（本事例では特殊なモデルを作成）



3. 形式手法の適用

3.5 検査項目と検査式の例

検査項目 ： CPUは暴走し続けない

⇩ CTL式に変換

事前変換 ： 「CPU状態 = 暴走状態」である状態が継続しない

CTL式 ： !EF (EG (CPU = boso))

EF(P) ： Exist Future(P)

将来Pとなることが在る

EG(Q) ： Exist Globally(Q)

ずっとQで在り続ける

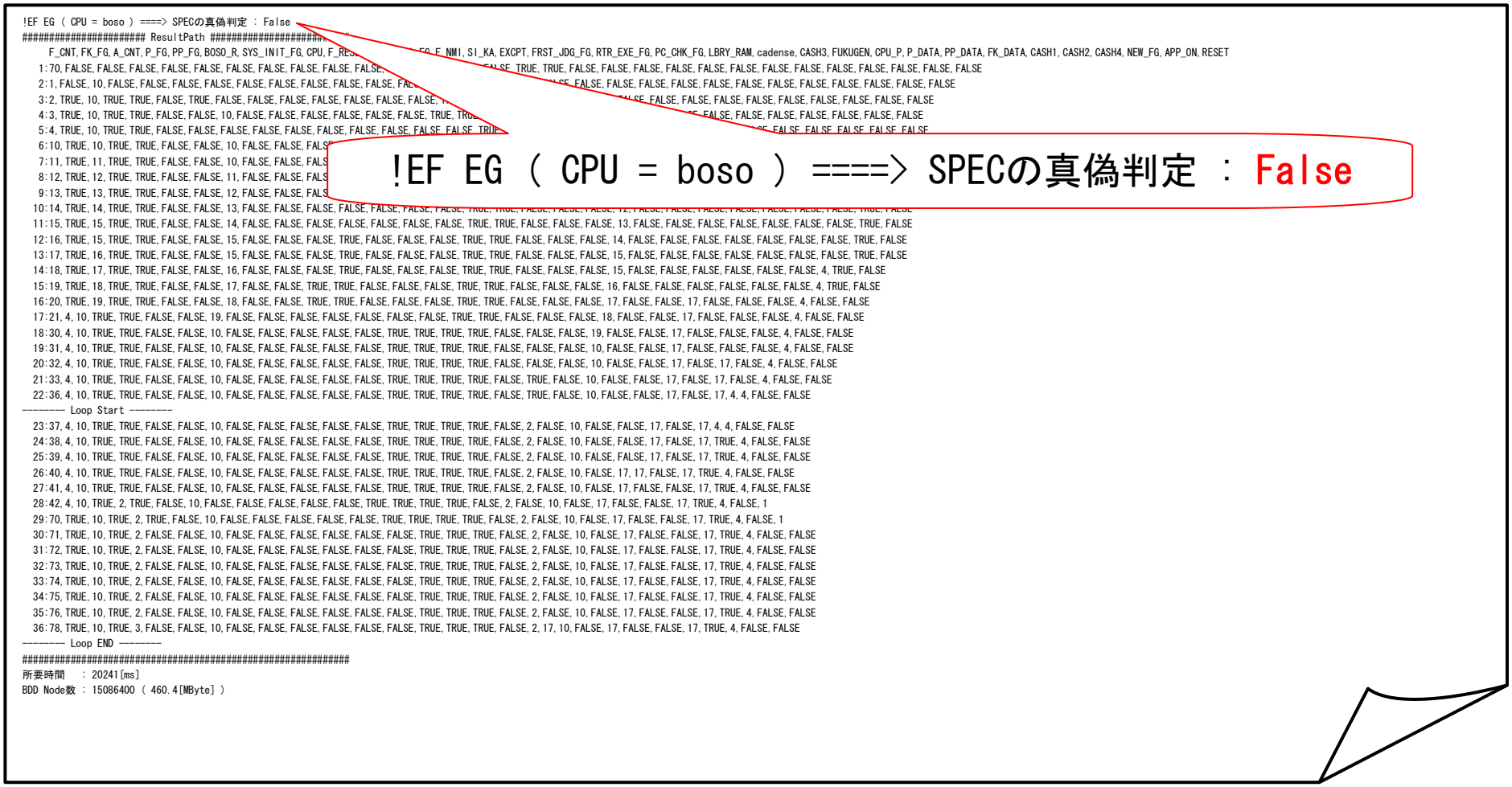
検査項目 → システム要件　満たすべき性質　正しい振る舞い
開発者／設計者が提示する（ドメイン知識が必要）

事前変換 → モデル検査の適用担当者が実施
CTL式 （モデル検査の知識が必要）

CTL:Computation Tree Logic
モデル検査器SMVで利用する検査式

3. 形式手法の適用

3.6 検査結果の紹介（反例_1）



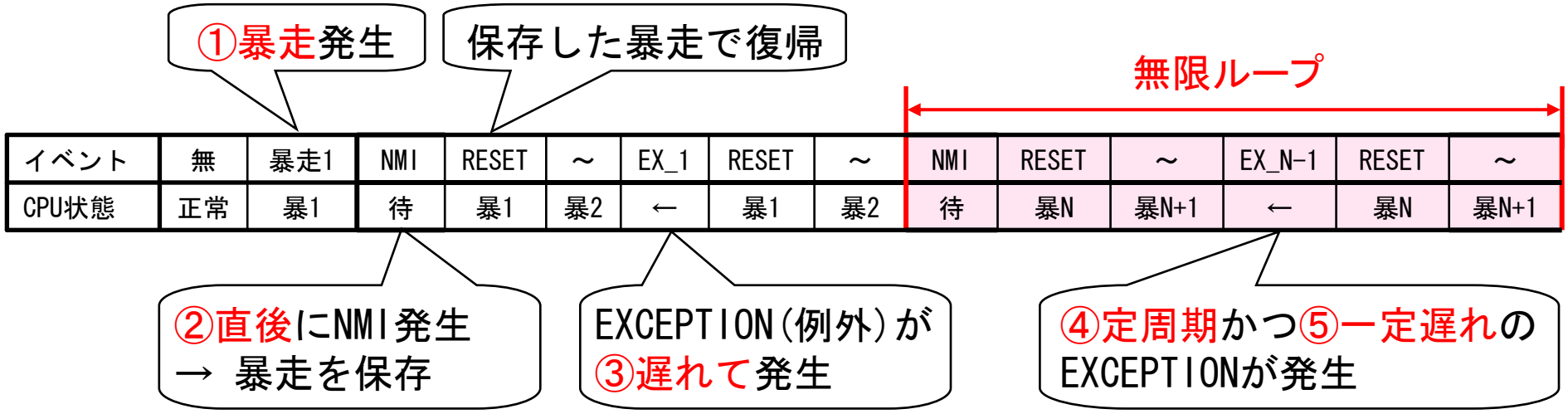

```
!EF EG ( CPU = boso ) ====> SPECの真偽判定 : False
###################### ResultPath ######################
     F_CNT,FK_FG,A_CNT,P_FG,PP_FG,BOSO_R,SYS_INIT_FG,CPU,F_RES...FG,F_NMI,SI_KA,EXCPT,FRST_JDG_FG,RTR_EXE_FG,PC_CHK_FG,LBRY_RAM,cadense,CASH3,FUKUGEN,CPU_P,P_DATA,PP_DATA,FK_DATA,CASH1,CASH2,CASH4,NEW_FG,APP_ON,RESET
   1:70,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,...FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE
   2:1,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,...SE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE
   3:2,TRUE,10,TRUE,TRUE,FALSE,TRUE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,...ALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE
   4:3,TRUE,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRU...,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE
   5:4,TRUE,10,TRUE,TRUE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE...,FALSE,FALSE,FALSE,FALSE,FALSE
   6:10,TRUE,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALS...
   7:11,TRUE,11,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALS...
   8:12,TRUE,12,TRUE,TRUE,FALSE,FALSE,11,FALSE,FALSE,FALS...
   9:13,TRUE,13,TRUE,TRUE,FALSE,FALSE,12,FALSE,FALSE,FALS...
  10:14,TRUE,14,TRUE,TRUE,FALSE,FALSE,13,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,13,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,FALSE
  11:15,TRUE,15,TRUE,TRUE,FALSE,FALSE,14,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,14,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,FALSE
  12:16,TRUE,15,TRUE,TRUE,FALSE,FALSE,15,FALSE,FALSE,FALSE,TRUE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,14,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,FALSE
  13:17,TRUE,16,TRUE,TRUE,FALSE,FALSE,15,FALSE,FALSE,FALSE,TRUE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,15,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,FALSE
  14:18,TRUE,17,TRUE,TRUE,FALSE,FALSE,16,FALSE,FALSE,FALSE,TRUE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,15,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,4,TRUE,FALSE
  15:19,TRUE,18,TRUE,TRUE,FALSE,FALSE,17,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,16,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,4,TRUE,FALSE
  16:20,TRUE,19,TRUE,TRUE,FALSE,FALSE,18,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,17,FALSE,FALSE,17,FALSE,FALSE,FALSE,4,FALSE,FALSE
  17:21,4,10,TRUE,TRUE,FALSE,FALSE,19,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,FALSE,FALSE,FALSE,18,FALSE,FALSE,17,FALSE,FALSE,FALSE,4,FALSE,FALSE
  18:30,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,FALSE,FALSE,19,FALSE,FALSE,17,FALSE,FALSE,FALSE,4,FALSE,FALSE
  19:31,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,FALSE,FALSE,10,FALSE,FALSE,17,FALSE,FALSE,FALSE,4,FALSE,FALSE
  20:32,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,FALSE,FALSE,10,FALSE,FALSE,17,FALSE,17,FALSE,4,FALSE,FALSE
  21:33,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,TRUE,FALSE,10,FALSE,FALSE,17,FALSE,17,FALSE,4,FALSE,FALSE
  22:36,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,TRUE,FALSE,10,FALSE,FALSE,17,FALSE,17,4,4,FALSE,FALSE
-------- Loop Start --------
  23:37,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,FALSE,17,FALSE,17,4,4,FALSE,FALSE
  24:38,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,FALSE,17,FALSE,17,TRUE,4,FALSE,FALSE
  25:39,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,FALSE,17,FALSE,17,TRUE,4,FALSE,FALSE
  26:40,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,17,FALSE,17,TRUE,4,FALSE,FALSE
  27:41,4,10,TRUE,TRUE,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  28:42,4,10,TRUE,2,TRUE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,FALSE,17,TRUE,4,FALSE,1
  29:70,TRUE,10,TRUE,2,TRUE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,1
  30:71,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  31:72,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  32:73,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  33:74,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  34:75,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  35:76,TRUE,10,TRUE,2,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,FALSE,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
  36:78,TRUE,10,TRUE,3,FALSE,FALSE,10,FALSE,FALSE,FALSE,FALSE,FALSE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,2,17,10,FALSE,17,FALSE,FALSE,17,TRUE,4,FALSE,FALSE
-------- Loop END --------
############################################################
所要時間    : 20241[ms]
BDD Node数 : 15086400 ( 460.4[MByte] )
```

検査結果が「FALSE」の場合に出力される反例ファイル

3. 形式手法の適用

3.6 検査結果の紹介（反例_2）

検査項目 ： CPUが暴走し続けないこと
↑
反例 ： CPUが暴走し続けることがある



5つの稀なイベントが連続して発生した場合にCPUが暴走し続けることが判明
→ FUJIMIでは対応しないことに決定
（EXCEPTIONは暴走直後に発生＆暴走の無限ループにはWatchDog Timerで対応）

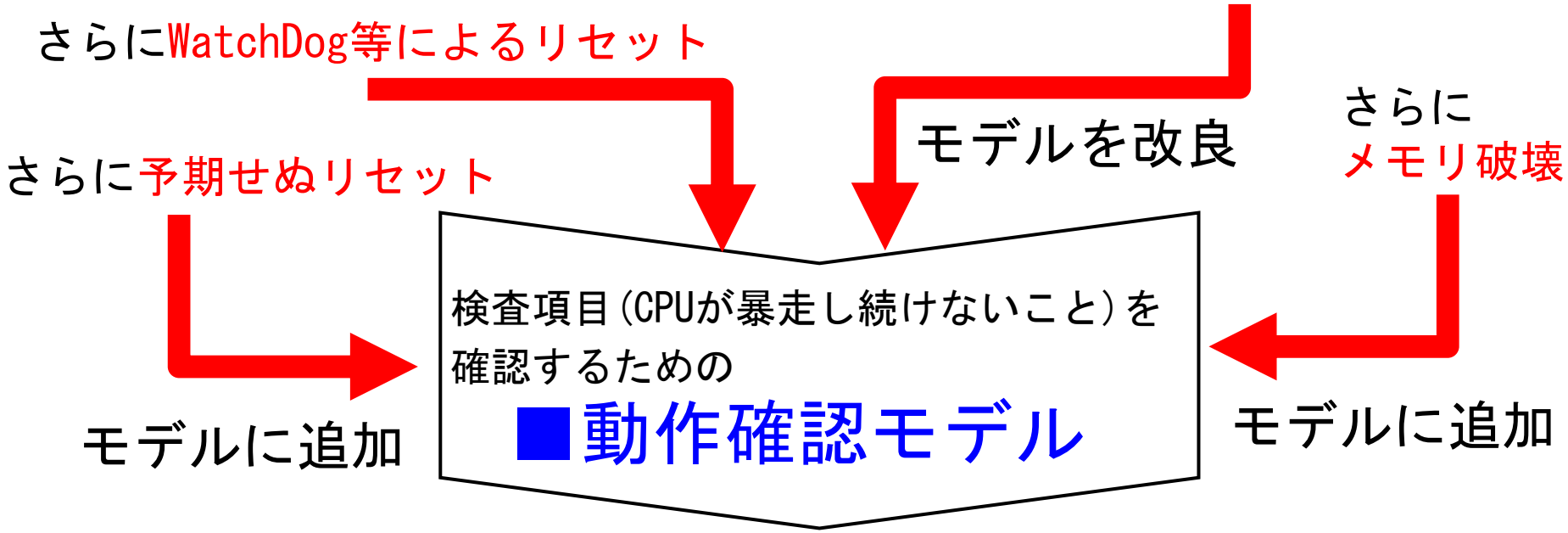
⇨ 設計の参考情報として提示

3. 形式手法の適用

3.7 最終の動作確認

前ページで・・・

→ FUJIMIでは対応しないことに決定（EXCEPTIONは暴走直後に発生する）

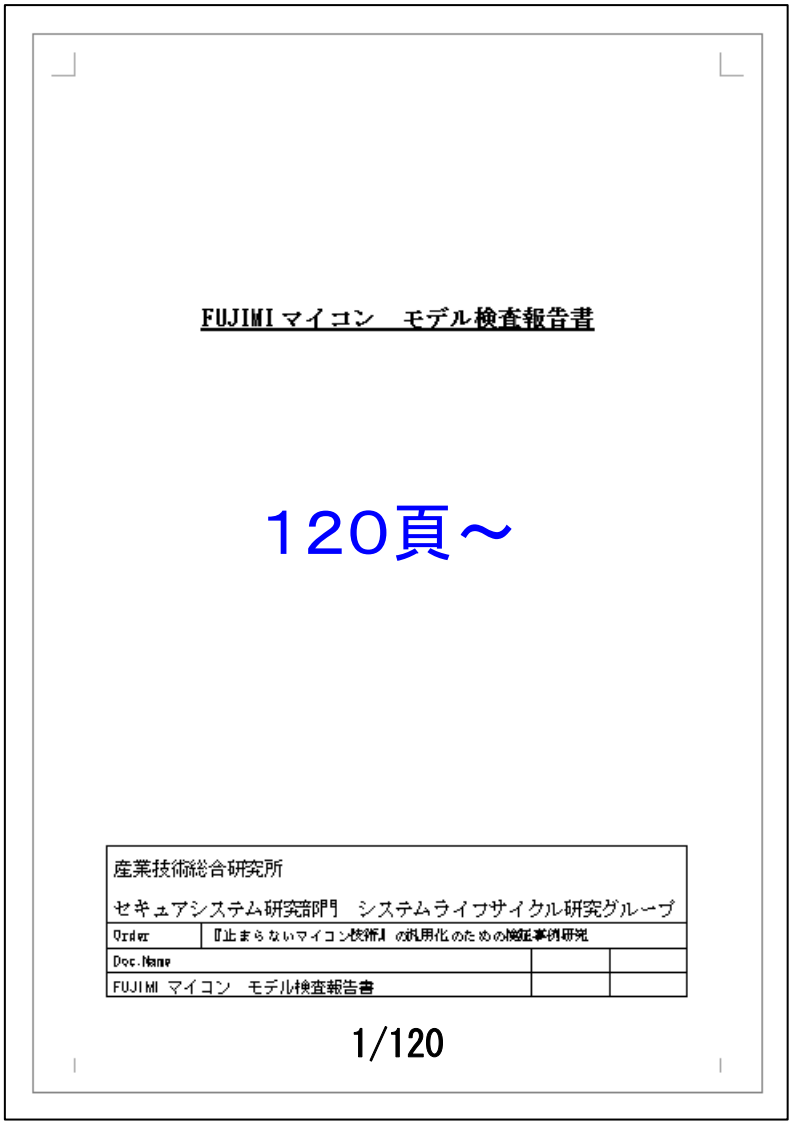



```
!EF EG ( CPU = boso ) ====> SPECの真偽判定 : True
所要時間    : 9112931[ms]
BDD Node数 : 530465968 ( 15.8[GByte] )
```

再検査 ： CPUが暴走し続けない ⇨ TRUE!!

3. 形式手法の適用

3.7 モデル検査報告書


FUJIMI マイコン　モデル検査報告書

120頁～

産業技術総合研究所

セキュアシステム研究部門　システムライフサイクル研究グループ

Order	『止まらないマイコン技術』の汎用化のための検証事例研究	
Doc.Name		
FUJIMI マイコン　モデル検査報告書		

1/120

【目次】