

# 統合的高信頼化設計のための モデル化と検出・訂正・回復技術

研究代表者 安浦 寛人

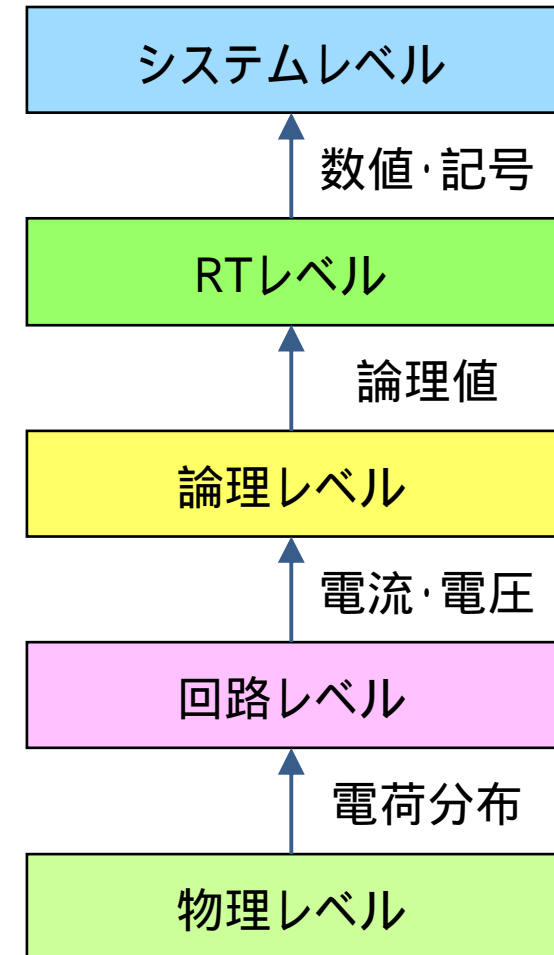
九州大学 大学院システム情報科学研究所

# 設計時におけるDependability評価技術

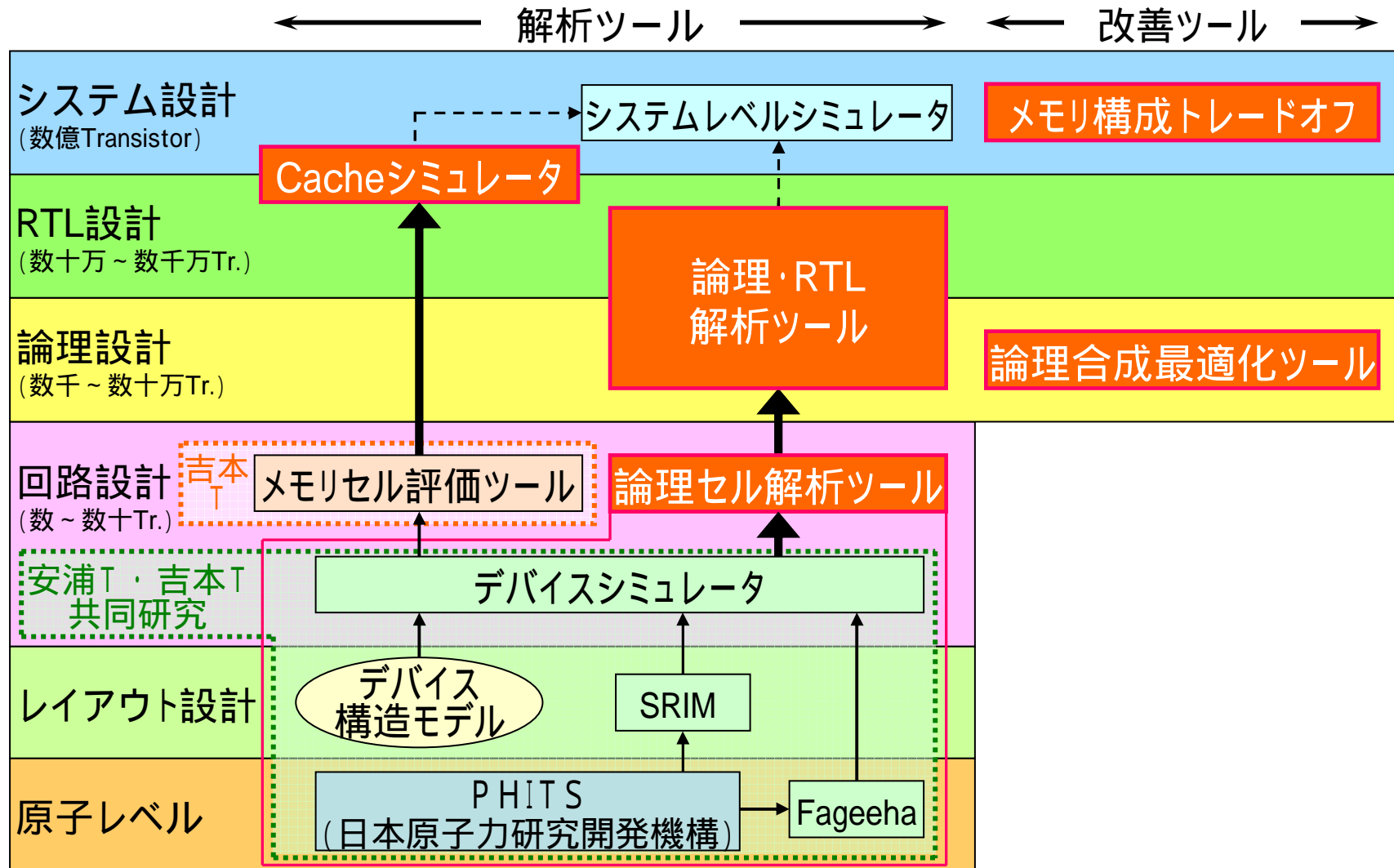
- VLSIシステムの設計は階層的に行われる。Dependabilityの評価も、この設計階層にあわせて構築するのが妥当である。
- 下位層のエラーは、上位層へ異なる信号形態で伝搬する。階層ごとにエラーのモデルの抽象度が異なり、その性質も異なる。
- 従来の技術は、各階層のモデルを独立に仮定し、その階層における評価だけを行っている。下位層の評価結果から上位層のエラーモデルを構築して評価する一貫した評価手法とそのためのツールチェーンの構築が必要である。

下位層におけるエラーの振る舞いを上位層の合理的なエラーモデルへ変換する技術  
階層が上がるごとに対象回路の規模が数十倍～千倍に増加するために、上位に行くほど評価のための計算量を押さえる工夫

最終的に、すべての階層を統合的に取り扱いシステムレベルでのDependabilityを評価する仕組みを構築する。

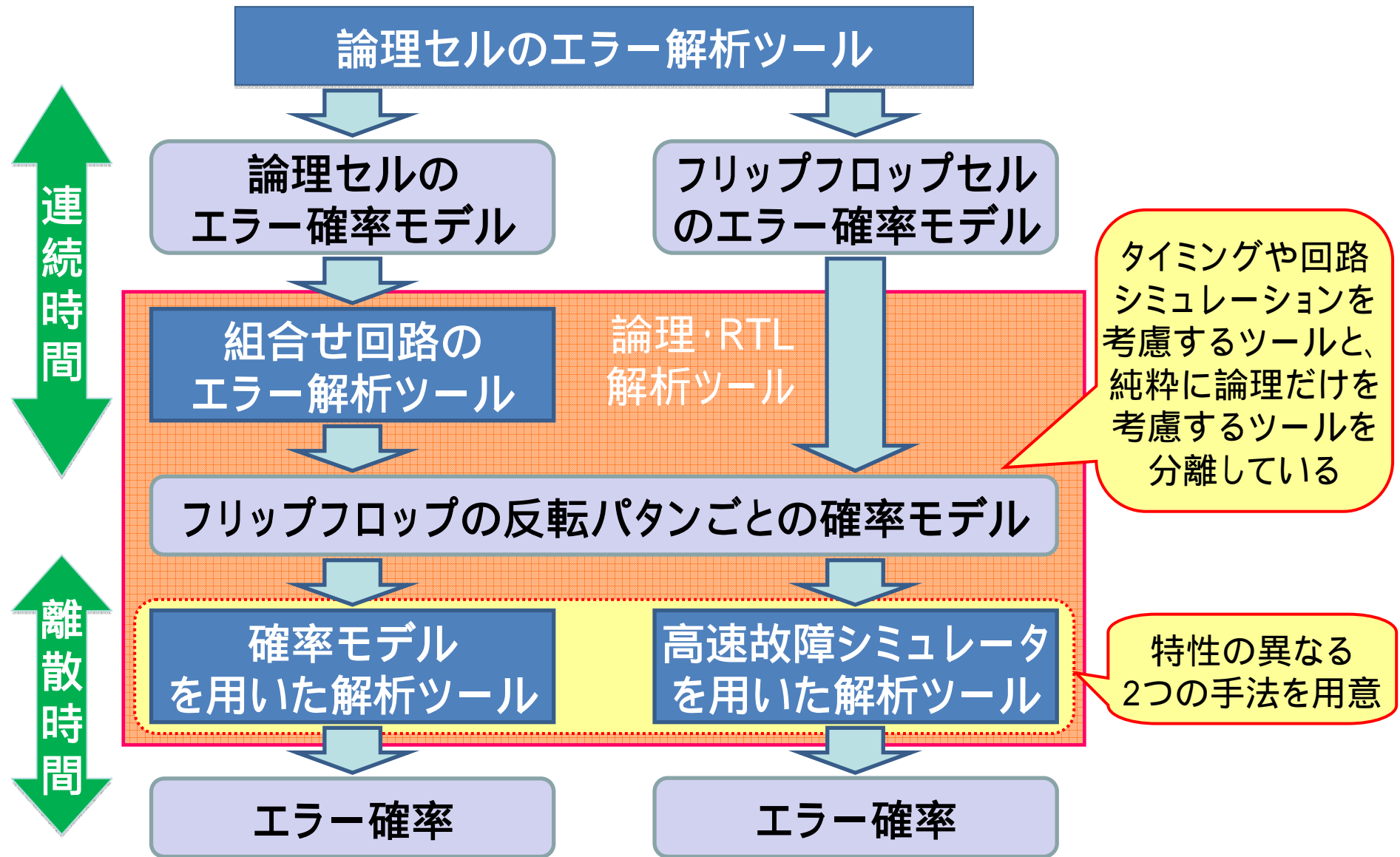


# ソフトウェアの 評価・解析ツールチェーン



	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

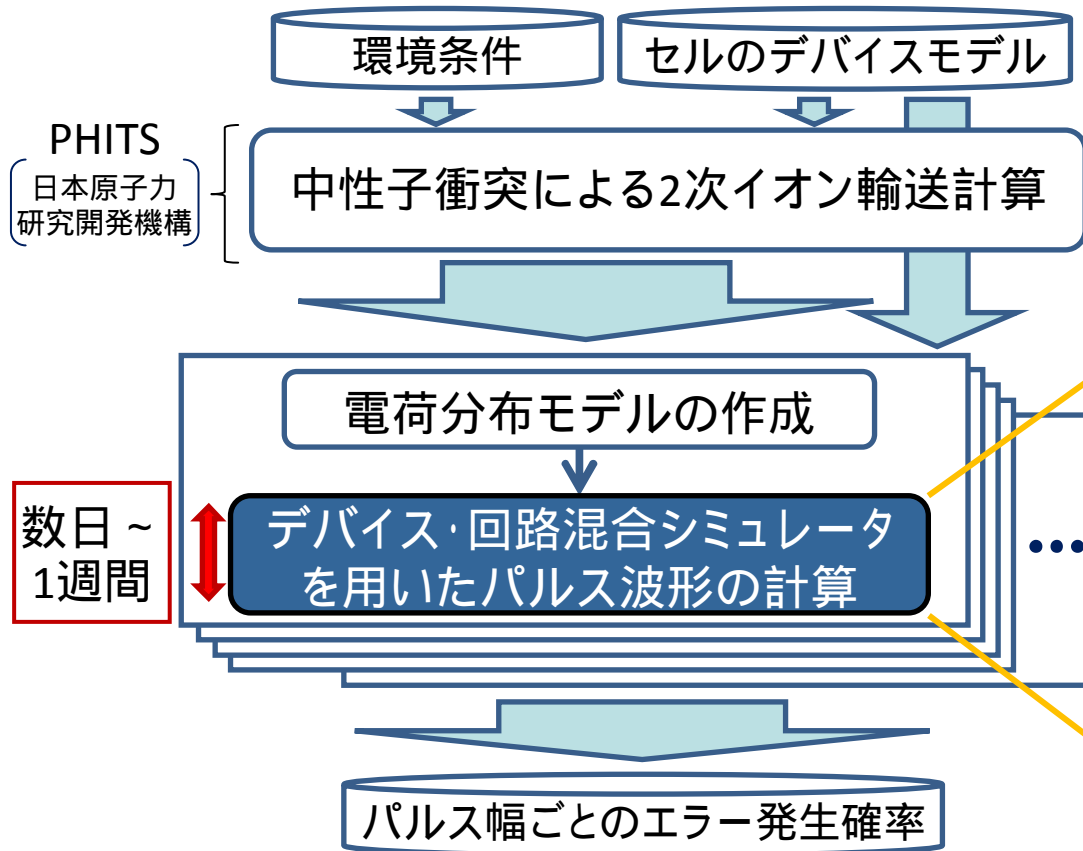
# エラーモデルと解析ツール



	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# 論理セルのエラー解析

## 新しいツールチェーン



数日 ~ 1週間

### 問題点

高い精度を得るためには十分な数のシミュレーションが必要

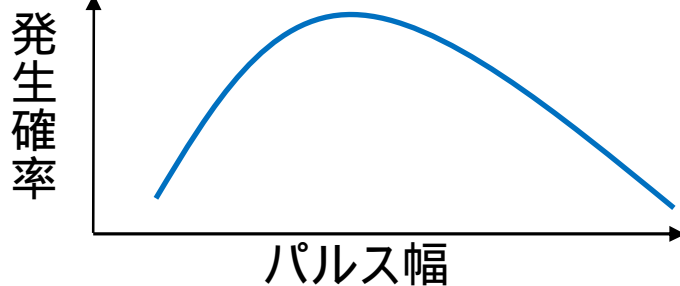
### 提案手法

領域ごとの収集電荷量を用いたノイズ電流モデルの近似

数秒

回路シミュレータを用いたパルス波形の計算

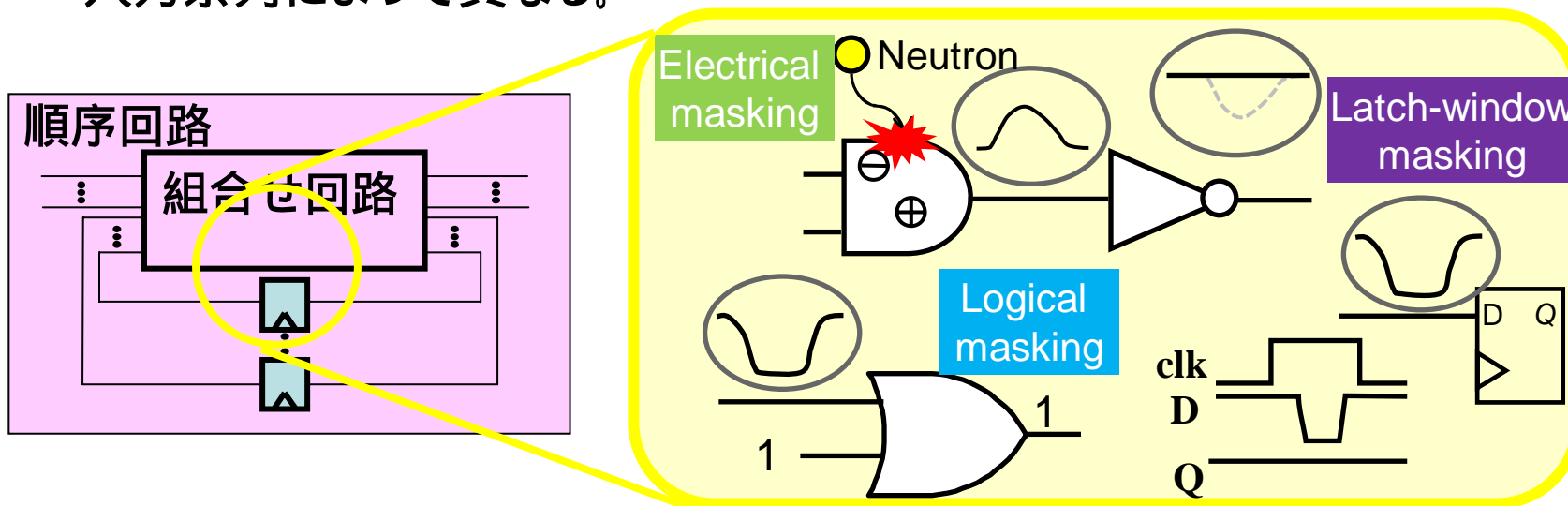
提案手法を用いることで数千から数万サンプルを1日で実行可能



	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# 論理・RTL解析の問題点

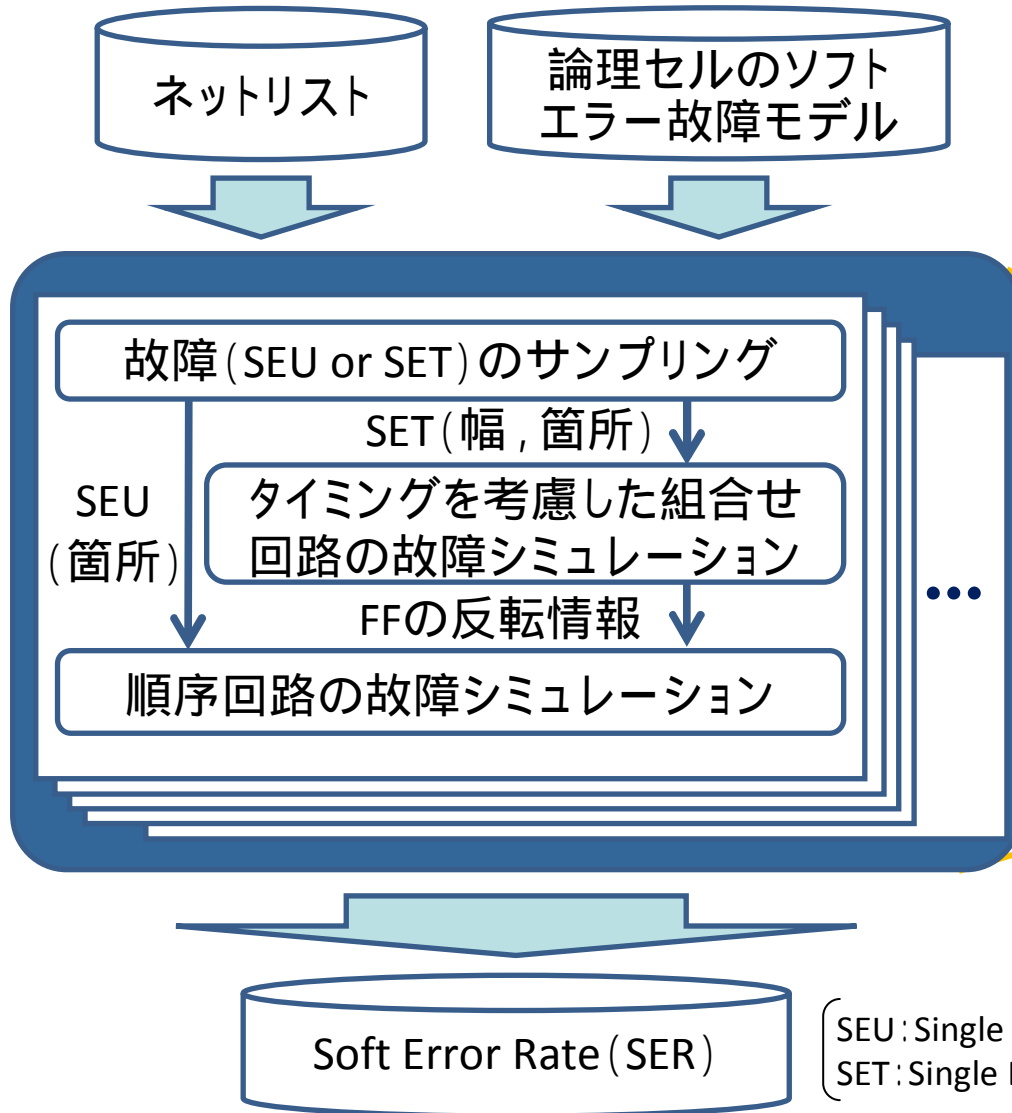
- 論理ゲート1つあたりのエラー確率 × 総ゲート数では  
組合せ回路のエラー確率は求められない。  
エラーの影響がマスクされることがある。  
マスクされるかどうかはエラーの種類によって異なる。
- 組合せ回路のエラー確率からフリップフロップを含んだ  
順序回路全体のエラー確率は求められない。  
マスクされるかどうかはフリップフロップ上のエラーパターンおよび  
入力系列によって異なる。



	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

# 論理・RTL解析ツール

## 新しいツールチェーン



## 問題点

- 単純な故障シミュレータを用いると、10万ゲート規模の回路に対して、1週間以上の処理時間が必要
- 十分な精度を得るためには数千から数万のサンプリングが必要

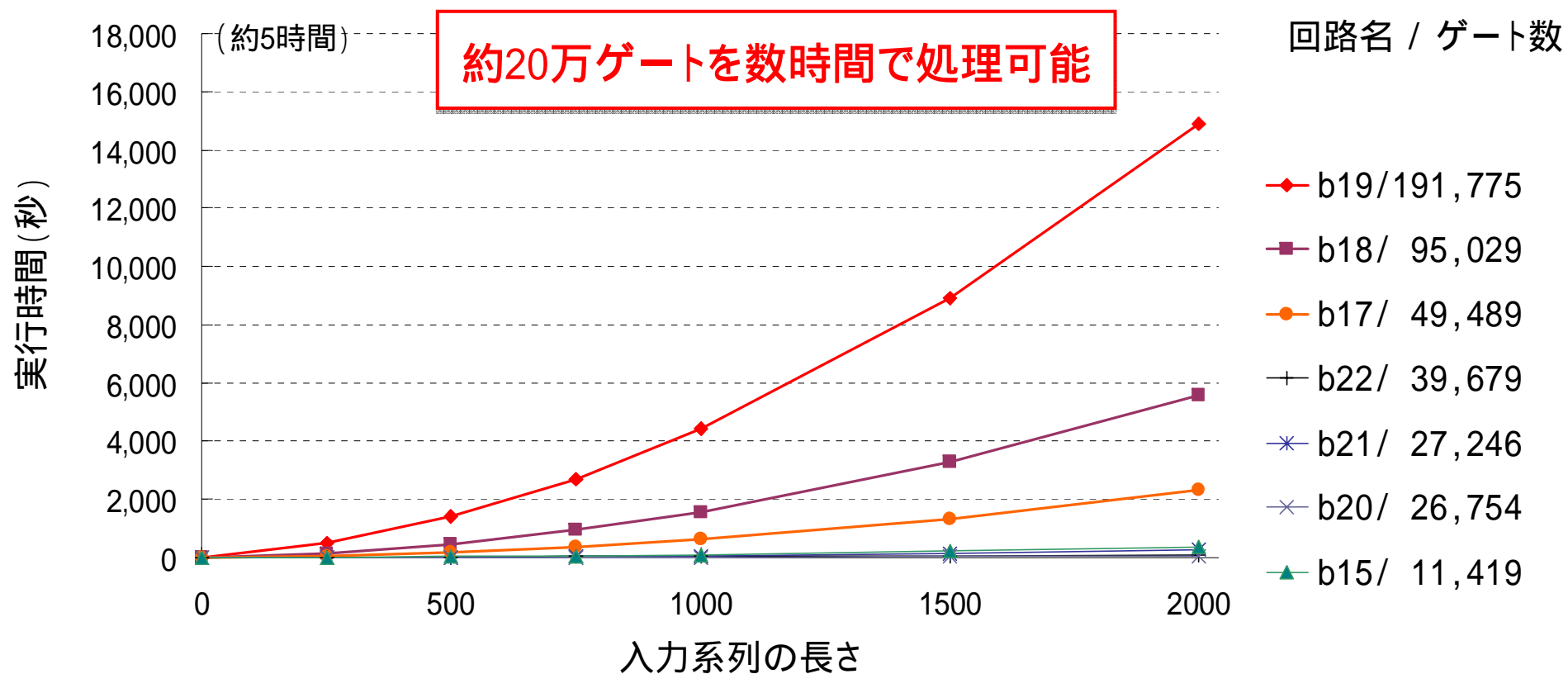
## 提案手法

- 全パターンを同時に考慮したタイミング故障シミュレーション
- 全セルを同時に考慮した組合せ回路故障シミュレーション
- 複数故障を同時に考慮した順序回路故障シミュレーション

上界を保証しつつ、10万ゲート規模の回路に対して、数時間で処理可能

	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

## 高速故障シミュレータの処理時間





	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

# 開発したツール

- 論理セルのエラー解析ツール  
デバイス構造と回路情報を用いて、パルス幅ごとの**エラー発生確率を計算**
- 組合せ回路のエラー解析ツール  
**エラー確率の上限を保証**しつつ、回路規模に比例した計算時間で処理を行う**近似アルゴリズム**
- 順序回路の確率モデルを用いた解析ツール  
与えられた**外部入力**の**確率分布のもとでの厳密値を保証**するアルゴリズム  
単純な手法に比べて計算時間を数十倍～数百倍高速化
- 順序回路の高速故障シミュレータを用いた解析ツール  
単純な手法に比べて**数百倍～千倍の高速化**を達成

	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

## 主要な成果1のまとめ

- 従来のLSIの設計フロー(ライブラリセルの設計と論理設計の分離、論理合成 + 自動配置配線の適用など)と親和性の高いツールチェーンを構築
- 今後の展開
  - より抽象度の高い、プロセッサの命令セットレベルや SystemC/SystemVerilog などのシステム記述レベルにおけるエラー解析へとシームレスにつなげるエラーモデルの構築

	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

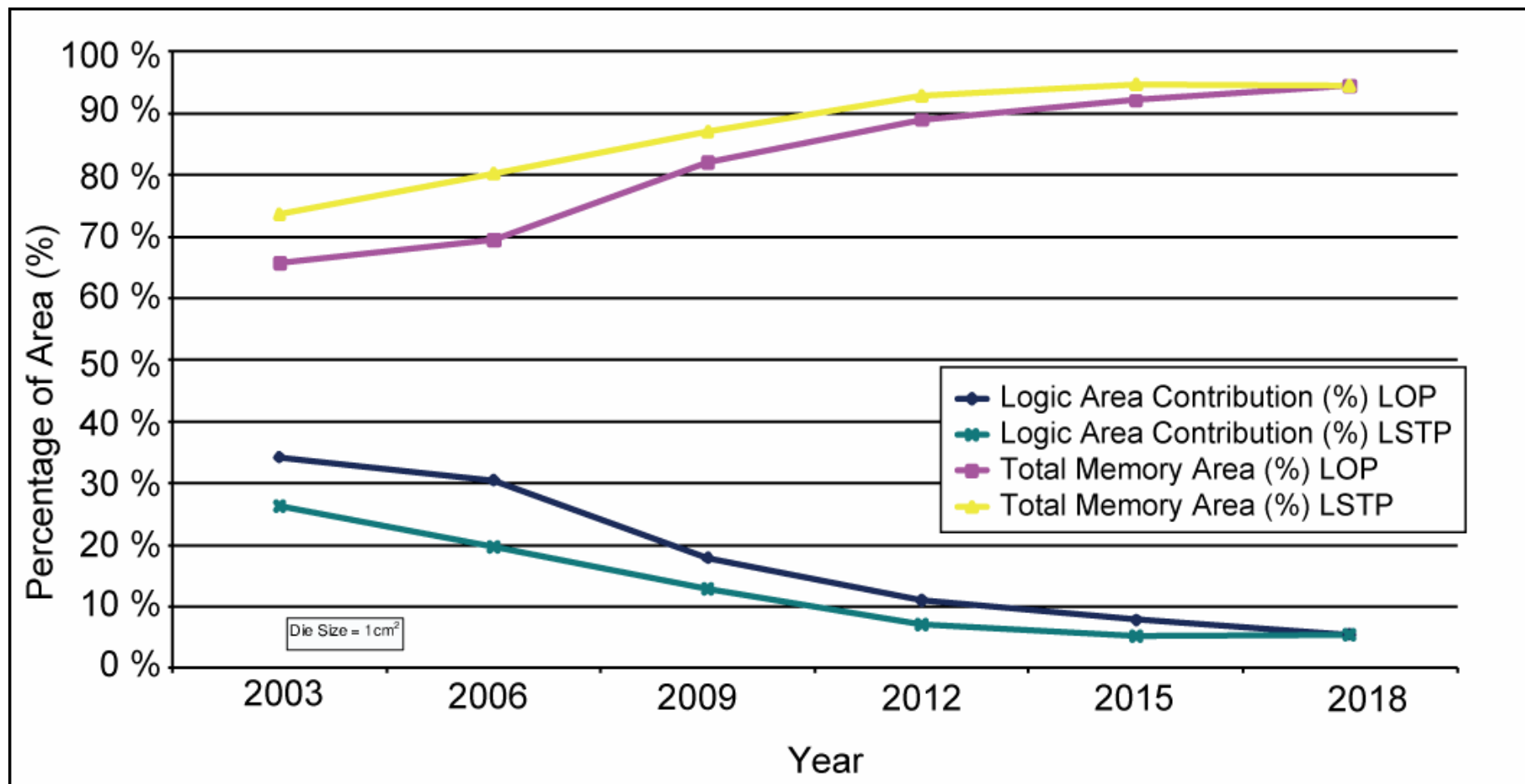
# システムレベルの キャッシュシミュレータ

- 種々のメモリ回路のセルのソフトエラー率から、プログラムの違いを考慮して、メモリシステムの脆弱性(ソフトエラー耐性の逆数)の変化を確認できるツール
- 計算時間(性能)やチップ面積と脆弱性のトレードオフを考慮したシステム設計が可能

システム設計者がDependabilityを他の設計制約や目標と同じように考慮して設計を行えるようになった

	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# ロジックとメモリの面積比率

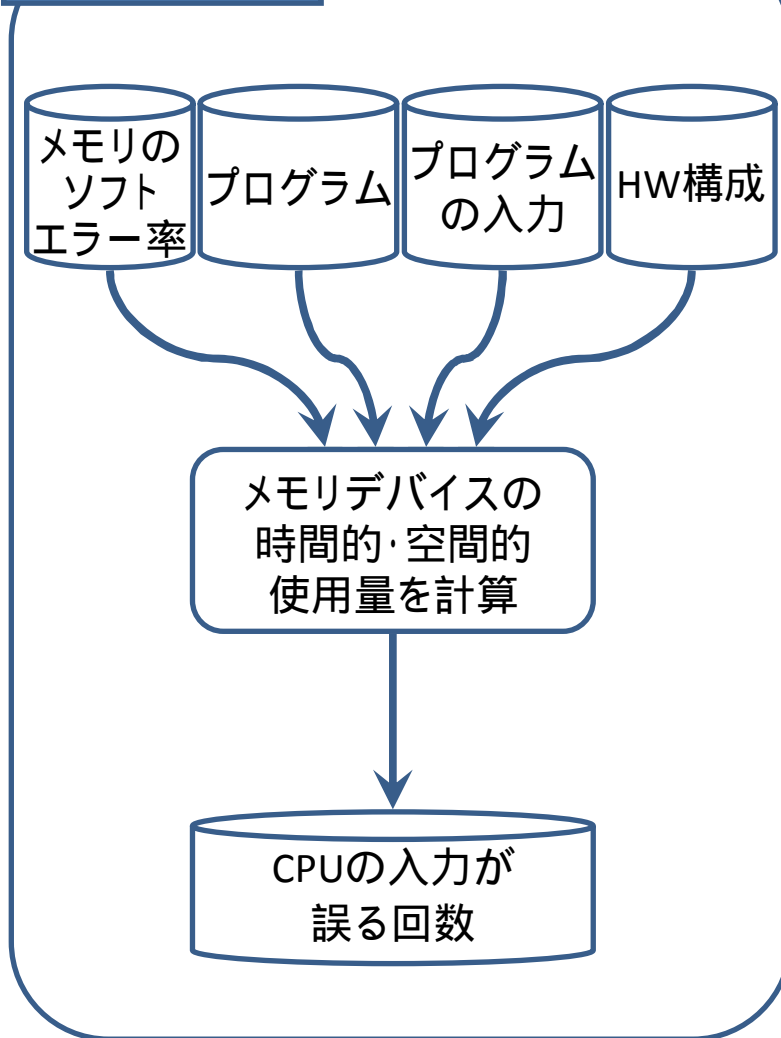


出典: ITRS 2003

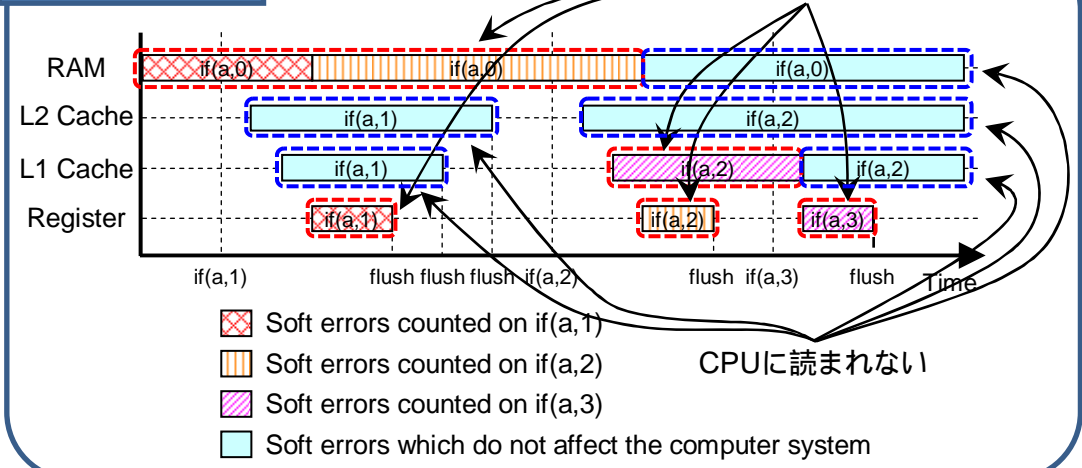
	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# キャッシュシミュレータ

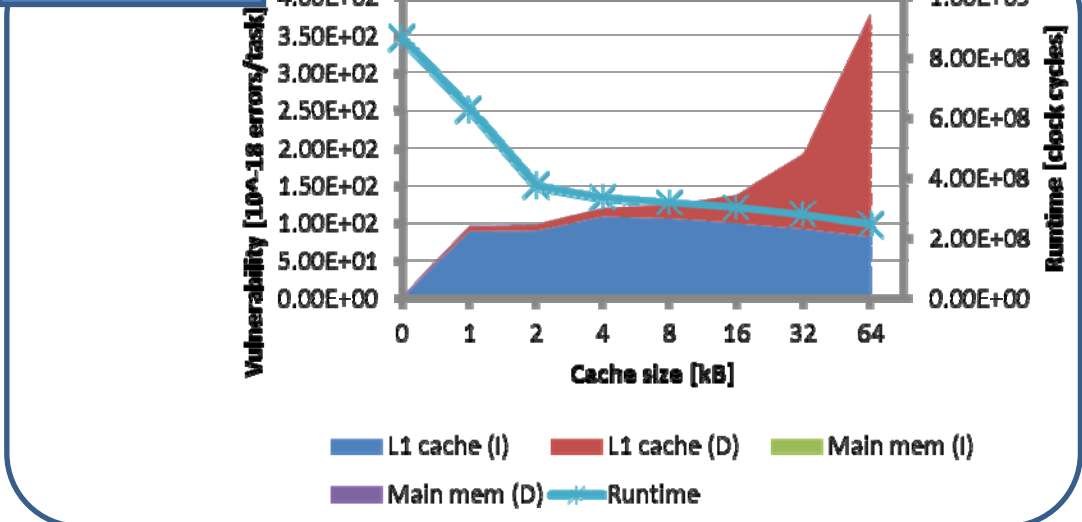
## 評価の流れ



## 評価方法



## 実験結果

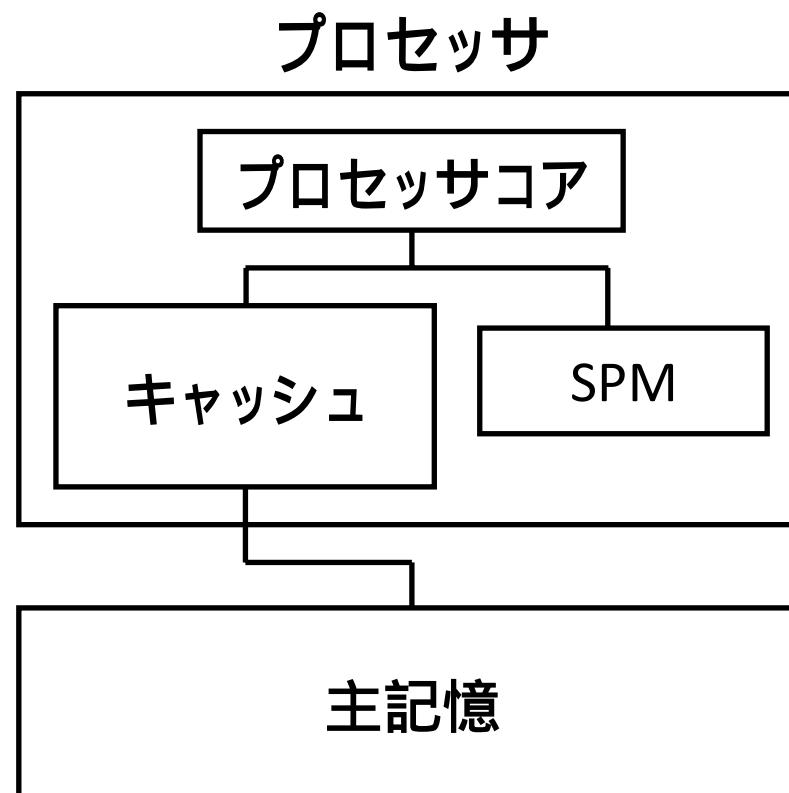


	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# スクラッチパッドメモリを用いた 組み込みシステムの高信頼化設計例

- キャッシュにはECC回路を実装しない
- ECC回路が実装されたスクラッチパッドメモリ (SPM) を付加

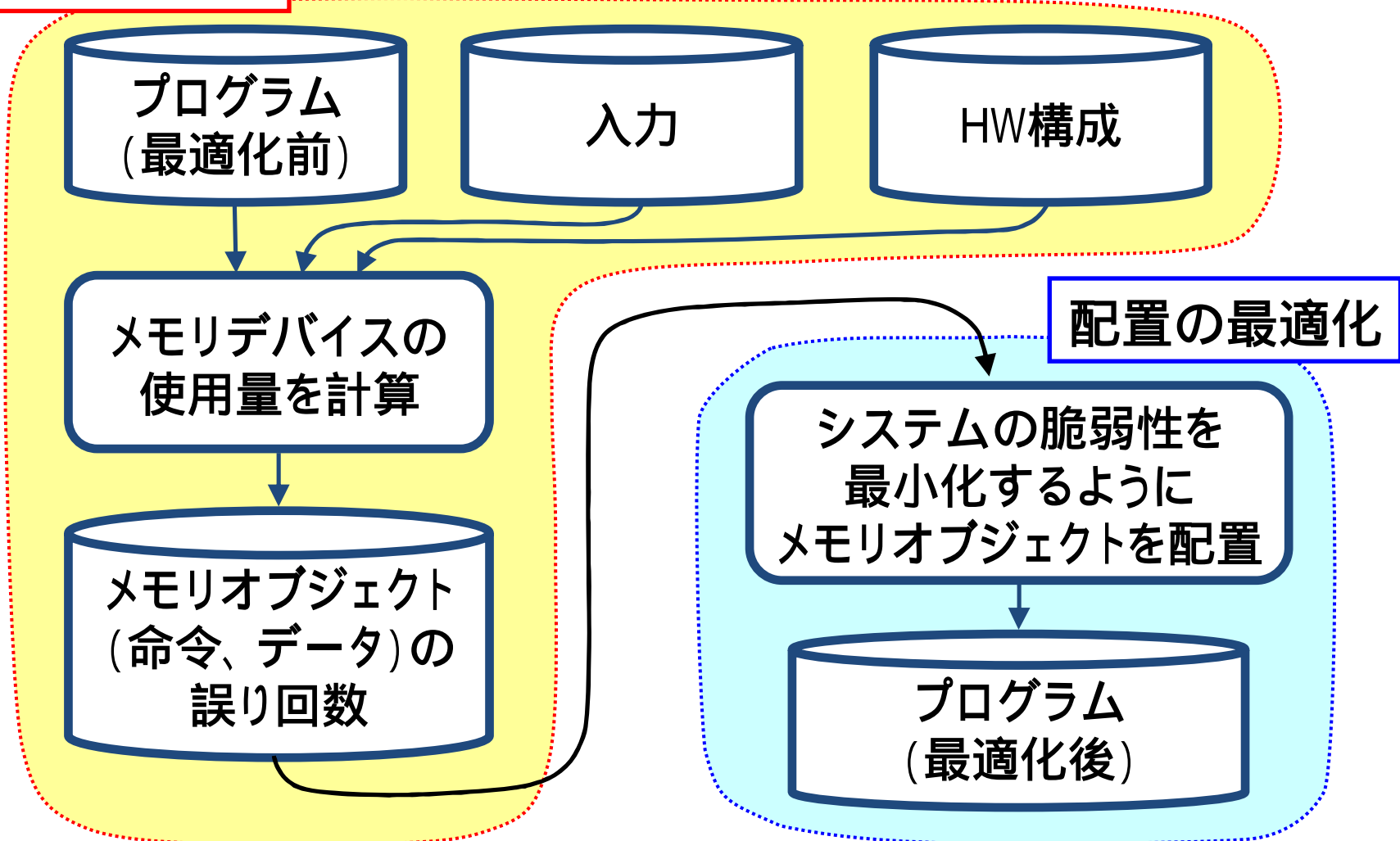
脆弱性が改善するように  
データや命令列を  
SPMや主記憶に配置



	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# メモリオブジェクト配置の戦略

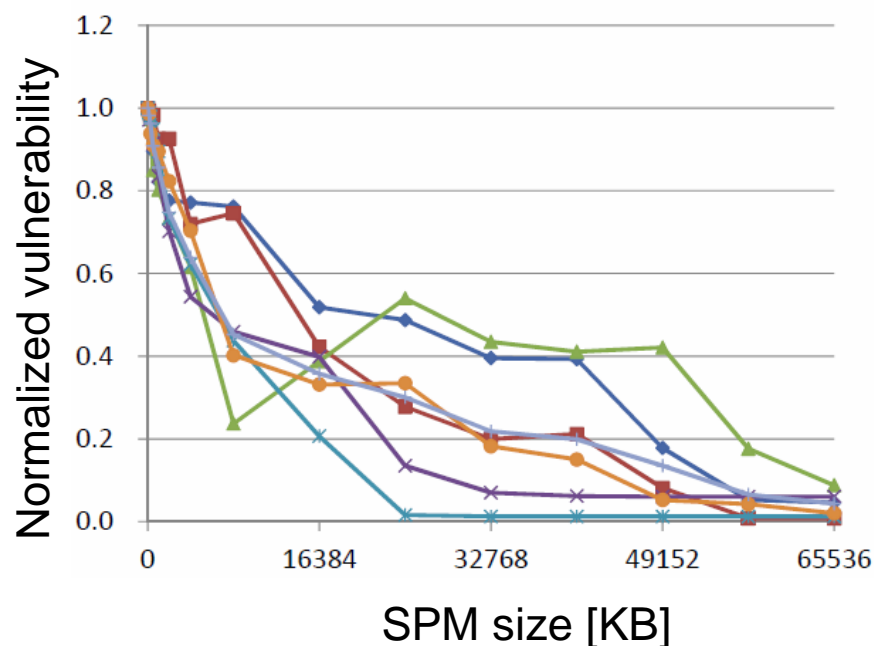
## 脆弱性の抽出



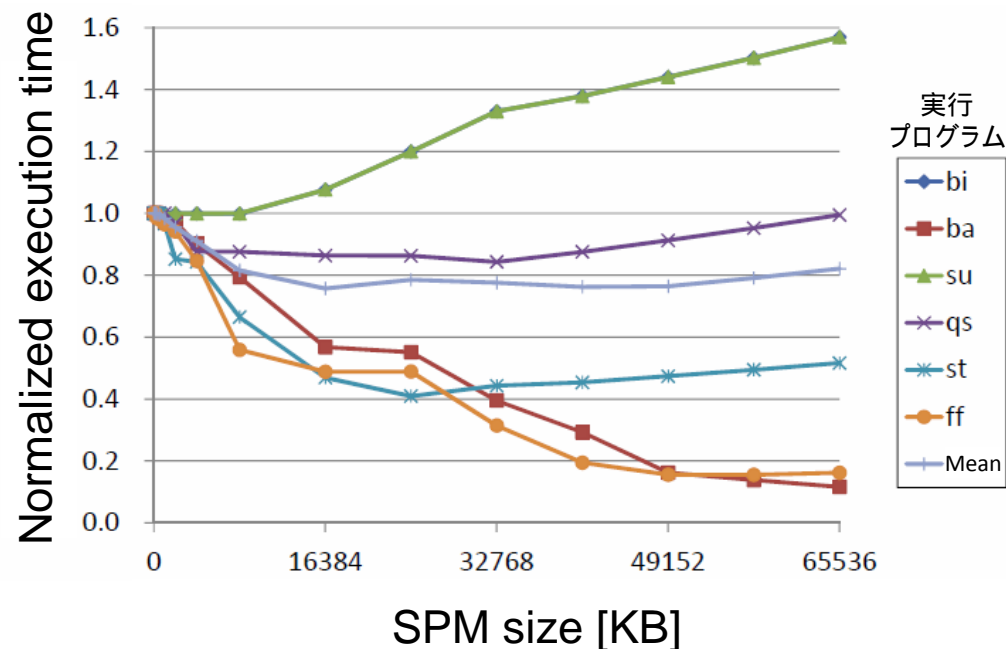
	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# スクラッチパッドメモリのサイズによる脆弱性と実行時間

Vulnerability (cache size: 16 KB)



Execution time (cache size: 16 KB)





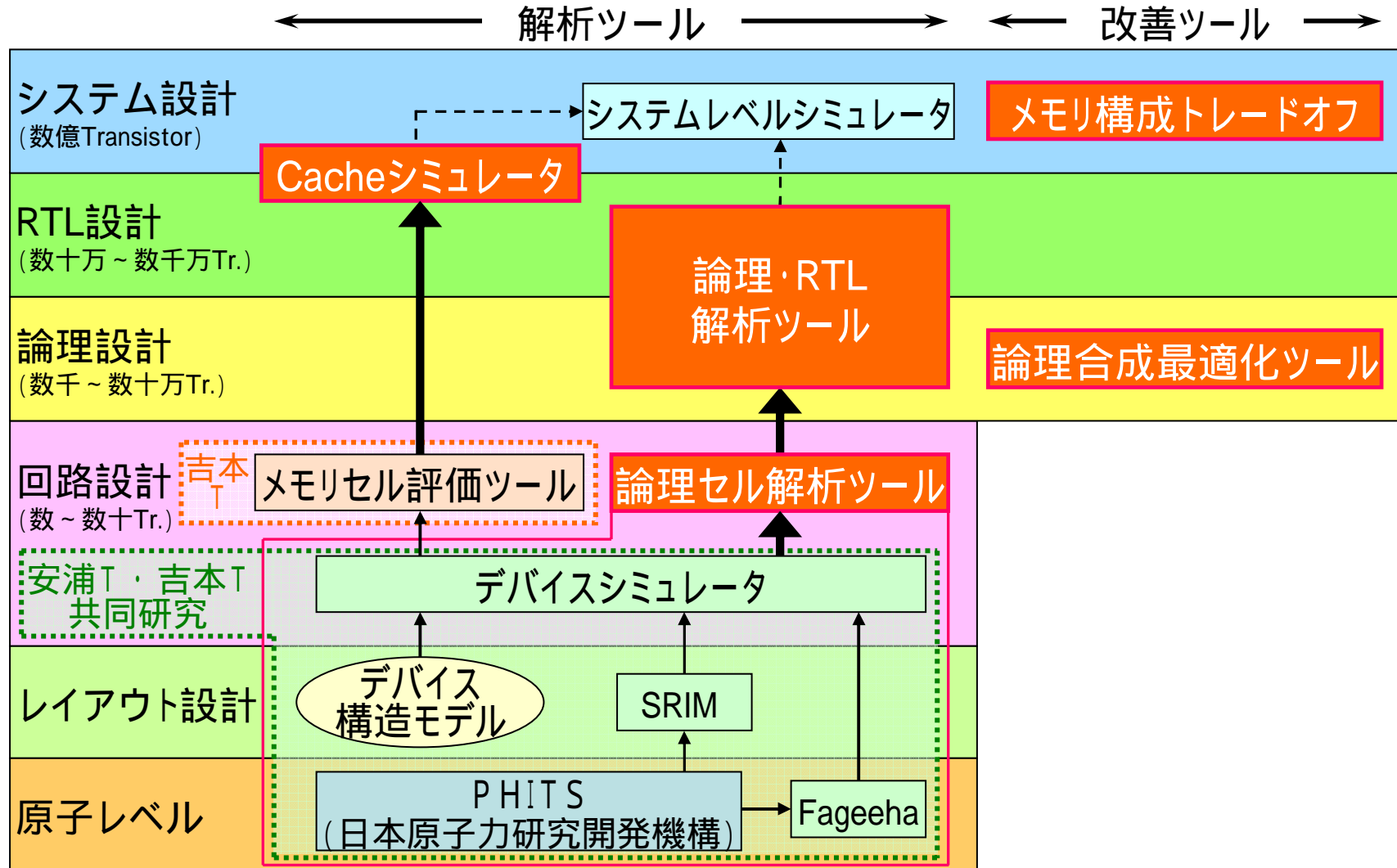
	論理回路	メモリ	システム
ソフトエラー			
タイミングエラー			
セキュリティ			

## 主要な成果2のまとめ

- **メモリセルのソフトエラー率**に基づいて、**CPUシステムの脆弱性**を評価するシミュレータの開発
- **脆弱性**と他の評価尺度(計算時間、チップ面積)との**トレードオフ**を図る設計技術
- 今後の展開  
論理回路の解析ツールとの連携

	論理回路	メモリ	システム
ソフトウェア			
タイミングエラー			
セキュリティ			

# ソフトウェアの 評価・解析ツールチェーン



# まとめ

1. **ディペンダブルVLSIの設計フローとツールチェーンの基本概念**
  - すべての階層を統合的に取り扱い、システムレベルでのDependabilityを評価する仕組みの構築
  - 3つのエラー要因(ソフトエラー、タイミングエラー、セキュリティ)の問題に対する検出・訂正・回復技術の開発
2. **中性子線等に起因するソフトエラーへの対応**
  - 設計者がDependabilityを考慮した設計を行えるようになった
3. **素子の製造ばらつきや経年劣化によるタイミングエラーへの対応**
  - カナリアFF考案:面積微減、エネルギー20%減、性能低下2%未満
  - 経年劣化軽減回路考案:SNM劣化25%改善、エネルギー増大5%未満
4. **悪意ある攻撃による回路内の機密データの漏洩への対応**
  - 「安全性vs.テスト容易性」「安全性vs.性能」のトレードオフ明示