

# 自動運転に向けたコード検証によるセキュリティ対策

**MathWorks Japan**

**アプリケーションエンジニアリング部 (制御)**

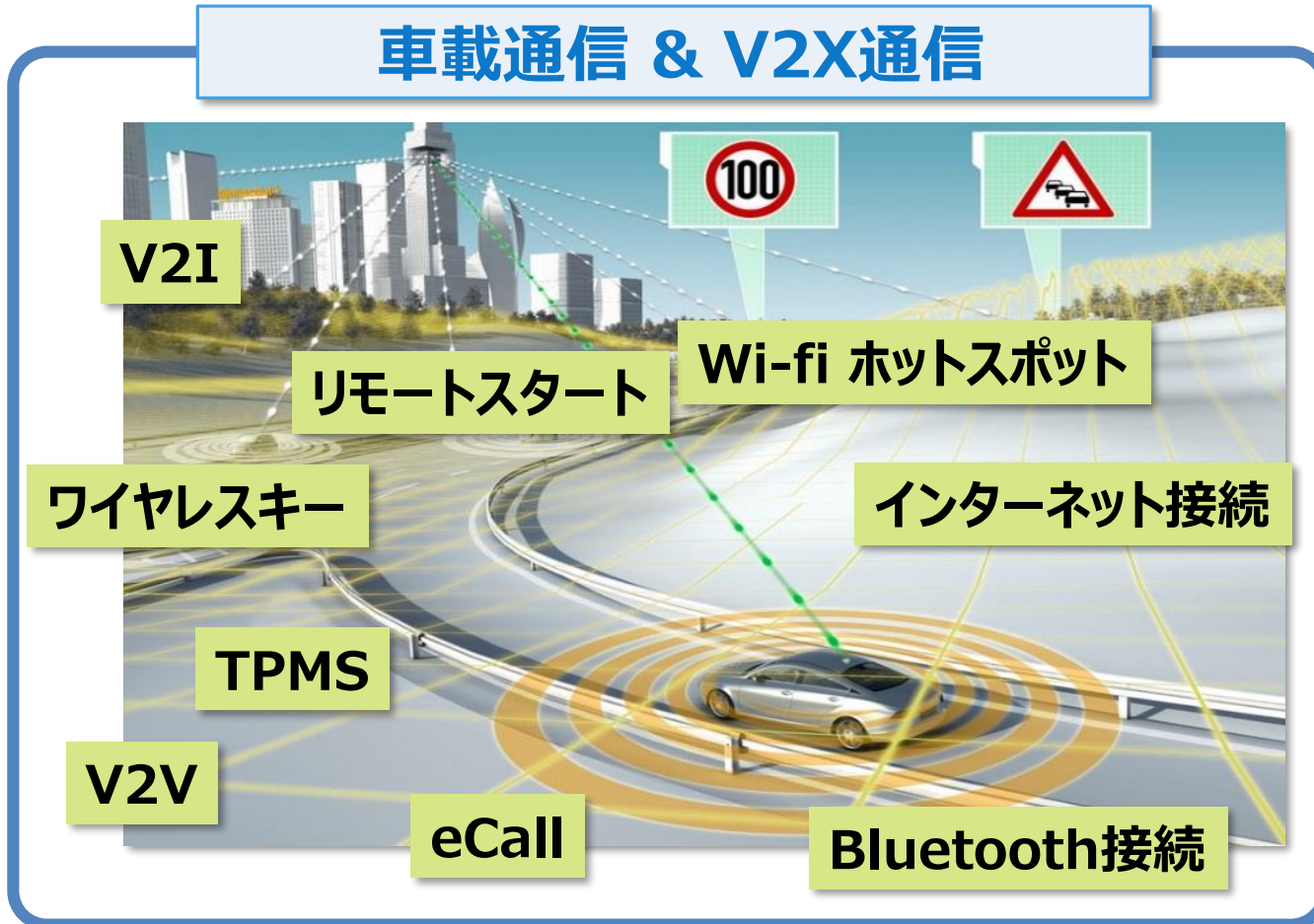
**アプリケーションエンジニア**

**田中 康博**

# 自動運転のサイバーセキュリティ

## ソフトウェアは安全性だけでなくセキュリティも重要

### 車載通信 & V2X通信



- 通信の増加
- インターネット上のノード
- サイバー攻撃の脅威にさらされる

安全性

セキュリティ

# 自動運転のサイバーセキュリティ (2)

## コードレベルでセキュリティを作り込むことが重要

### ソフトウェアの脆弱性：

Jeepハック後に140万台をリコール



出典：2015年  
<http://www.blogcdn.com/www.autoblog.com/media/2013/02/2014-jeep-cherokee-1.jpg>

セキュリティ強化後も  
ハッキング可能だった

出典：2017年  
<http://techon.nikkeibp.co.jp/atcl/column/15/425482/072800280/?P=3>



### セキュリティ対策を困難にする要因：

- H/WとS/Wのスペック
- セキュリティに対する知識
- セキュリティレベルの差

コードのセキュリティを  
何で検証するのか？



# Polyspace® – ソフトウェアのコード静的解析ソリューション

## コードのセキュリティと安全性の確保は静的解析が有効な手段

**Polyspace Bug Finder™**  
による**セキュリティ脆弱性の検出**



**Polyspace Code Prover™**  
による**安全性の証明**



# アジェンダ

## 1. サイバー攻撃の事例紹介

## 2. セキュリティ脆弱性の検出

## 3. ソフトウェアの安全性の証明


## 4. ユーザー事例 & まとめ

# Jeepハック



**HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT**



Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep drove it around an empty parking lot.  WHITNEY CURTIS FOR WIRED



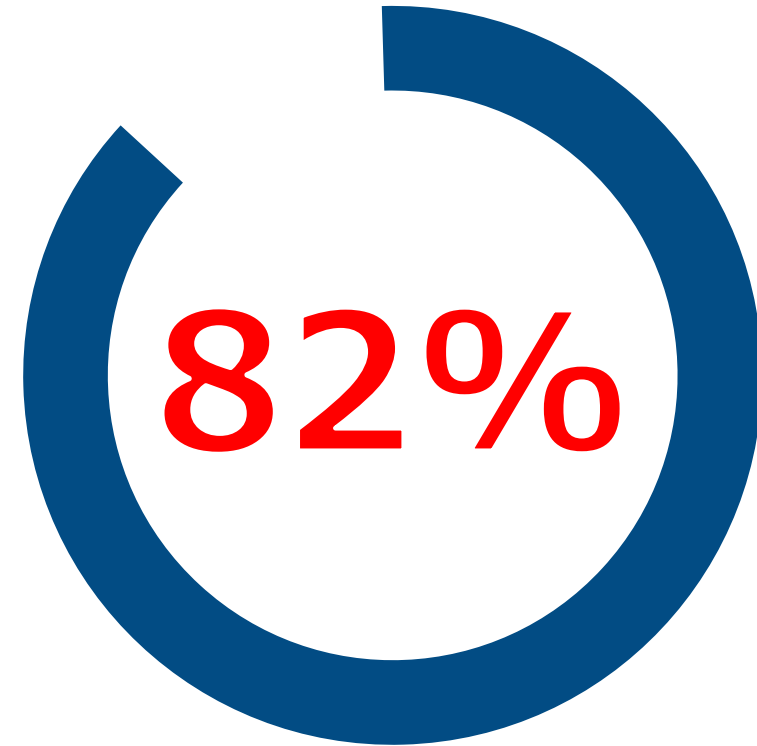
出典: 2015年 <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>

# 自動車のハッキングについての消費者の意識

## 消費者はセキュリティを重要視している



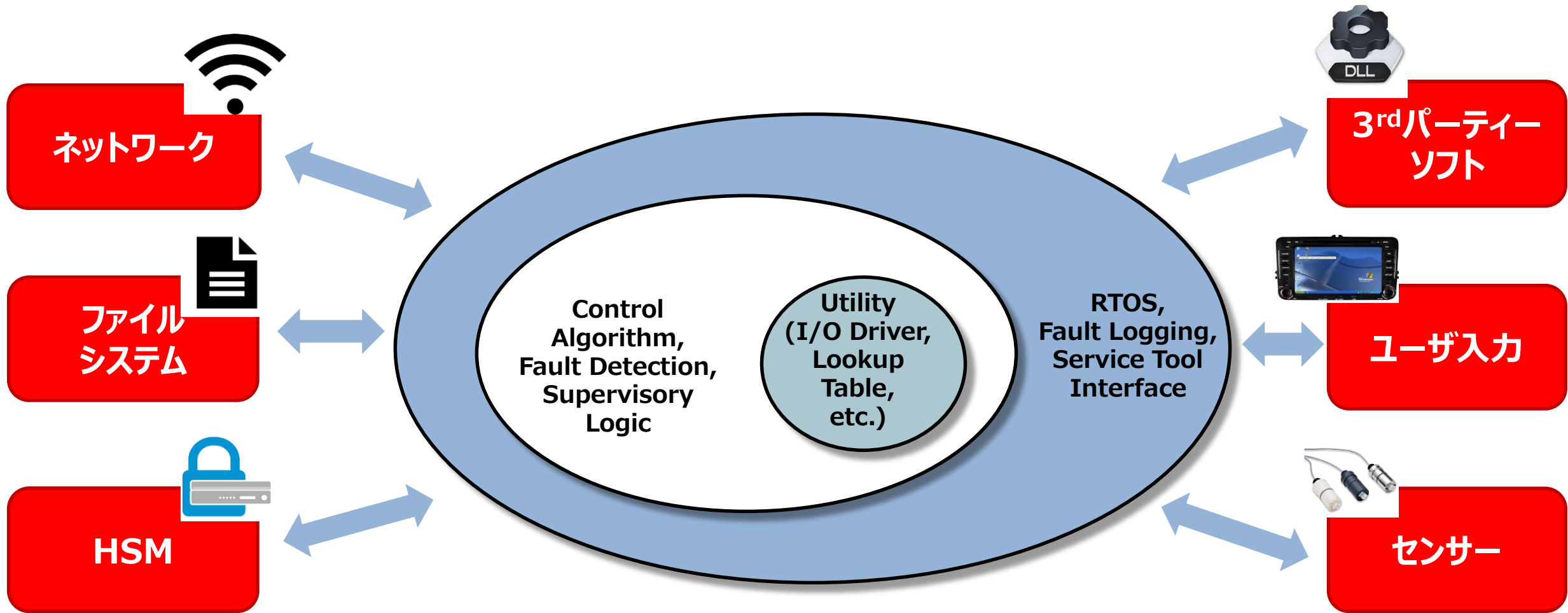
今後5年以内に自分の車が  
ハッキングされる可能性を心配している



もしハッキングされたら、その自動車  
メーカーから2度と購入しない

# 組み込みソフトウェアのセキュリティ – 外部インターフェース

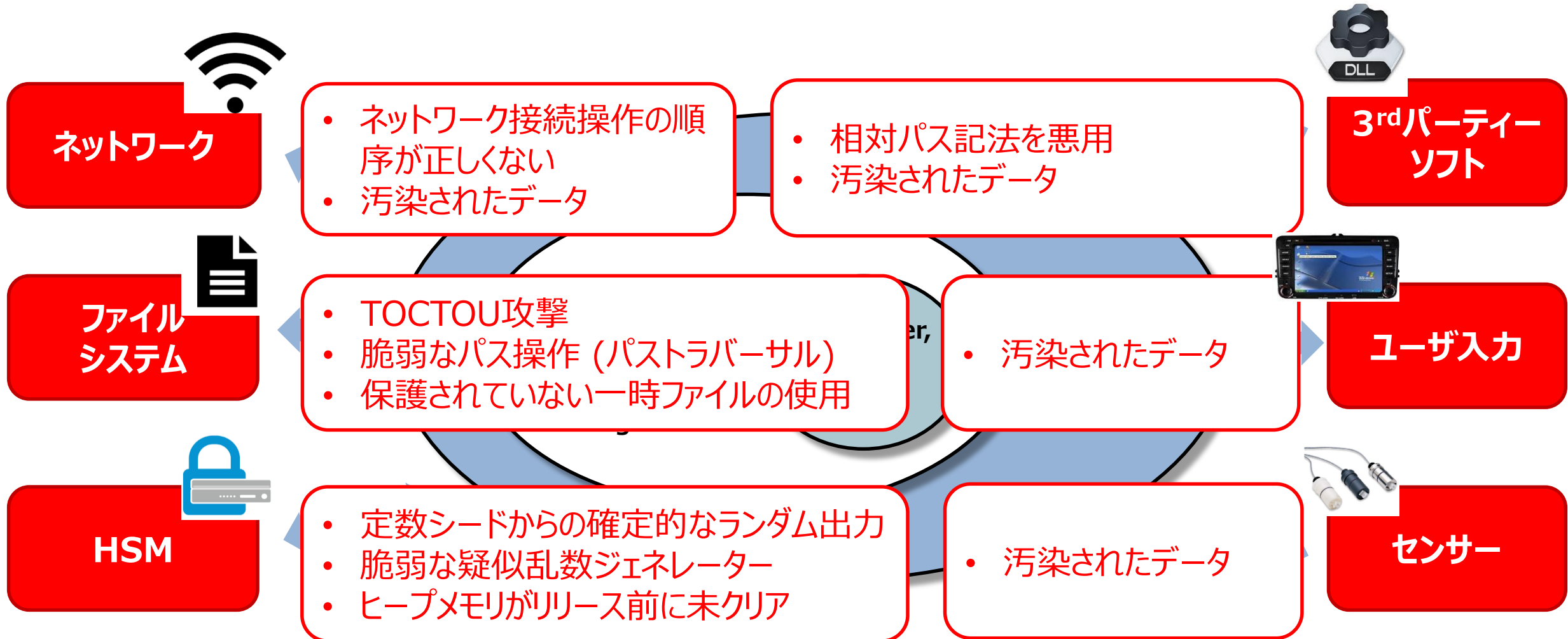
## 外部インターフェースを介して攻撃されるリスクが高まっている



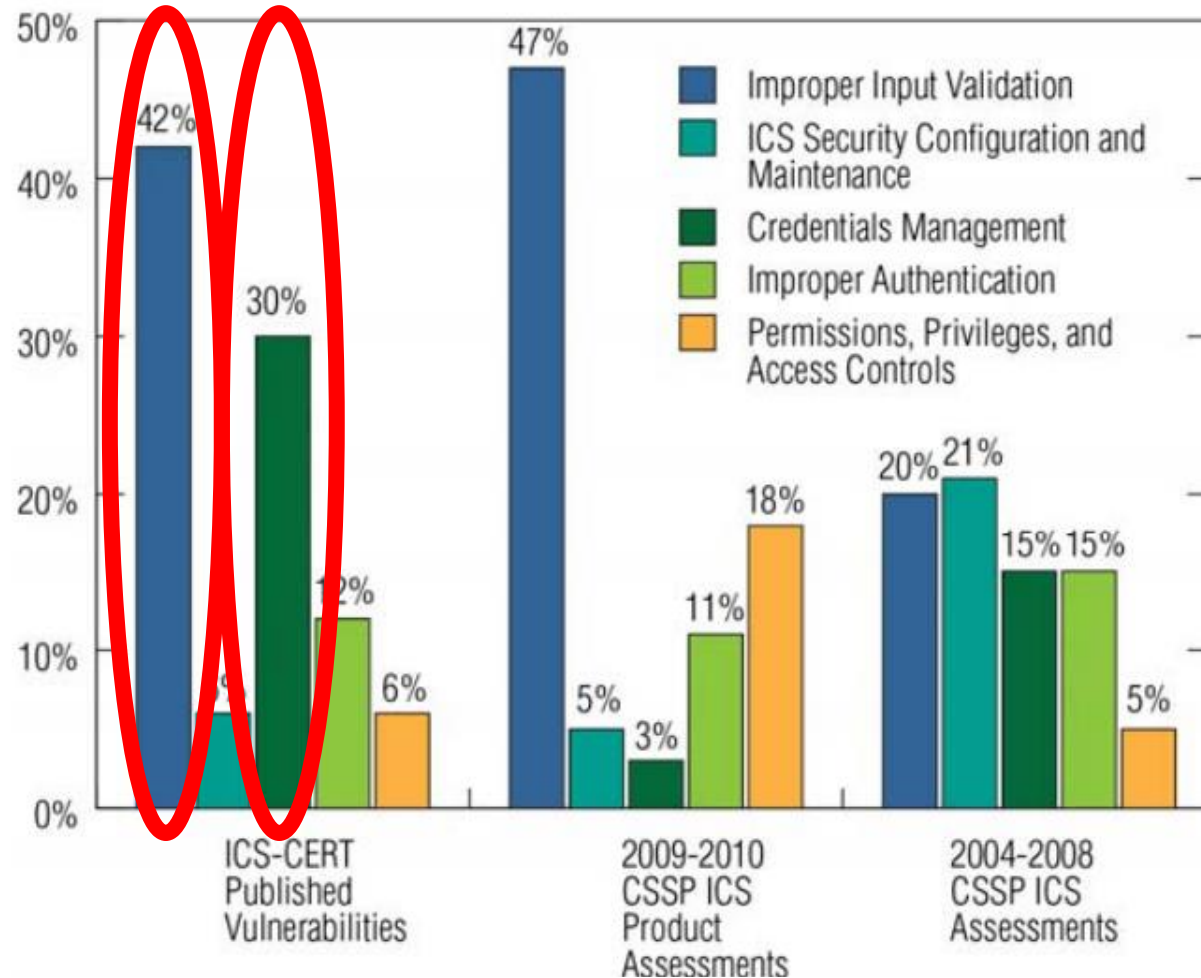


# 組み込みソフトウェアのセキュリティ – 脆弱性

## 外部インターフェースが多ければ攻撃されるリスクは更に高まる



# 組み込みソフトウェアのセキュリティ脆弱性

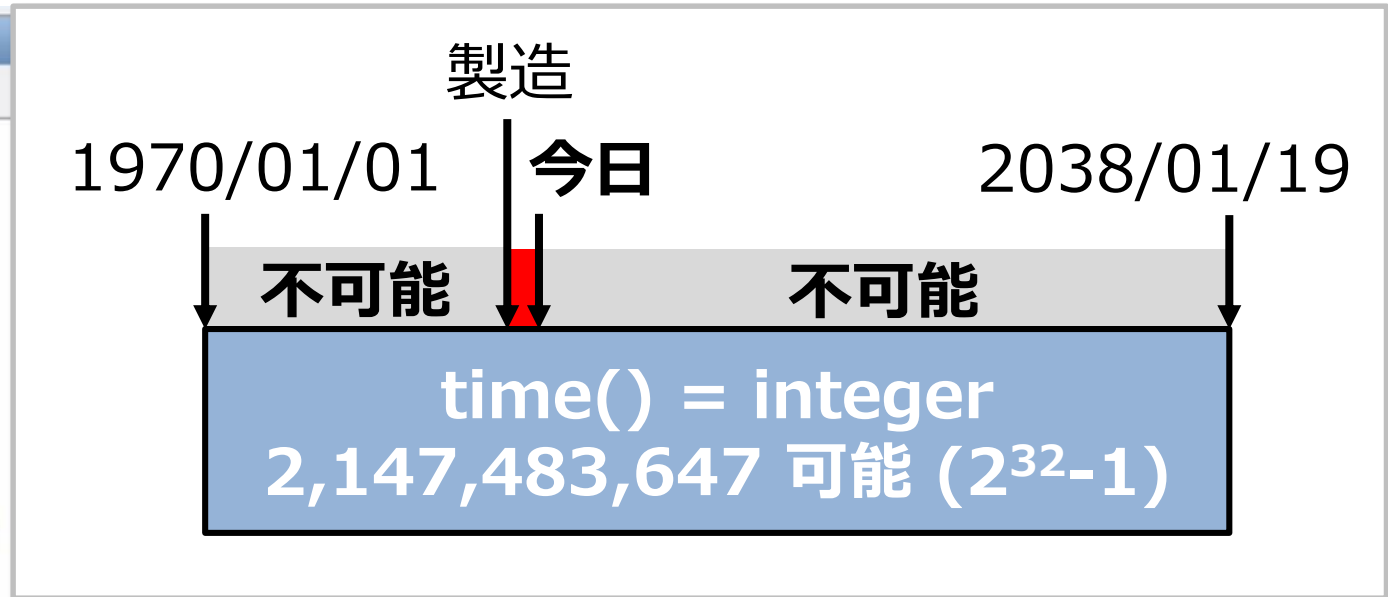


## 最大の問題:

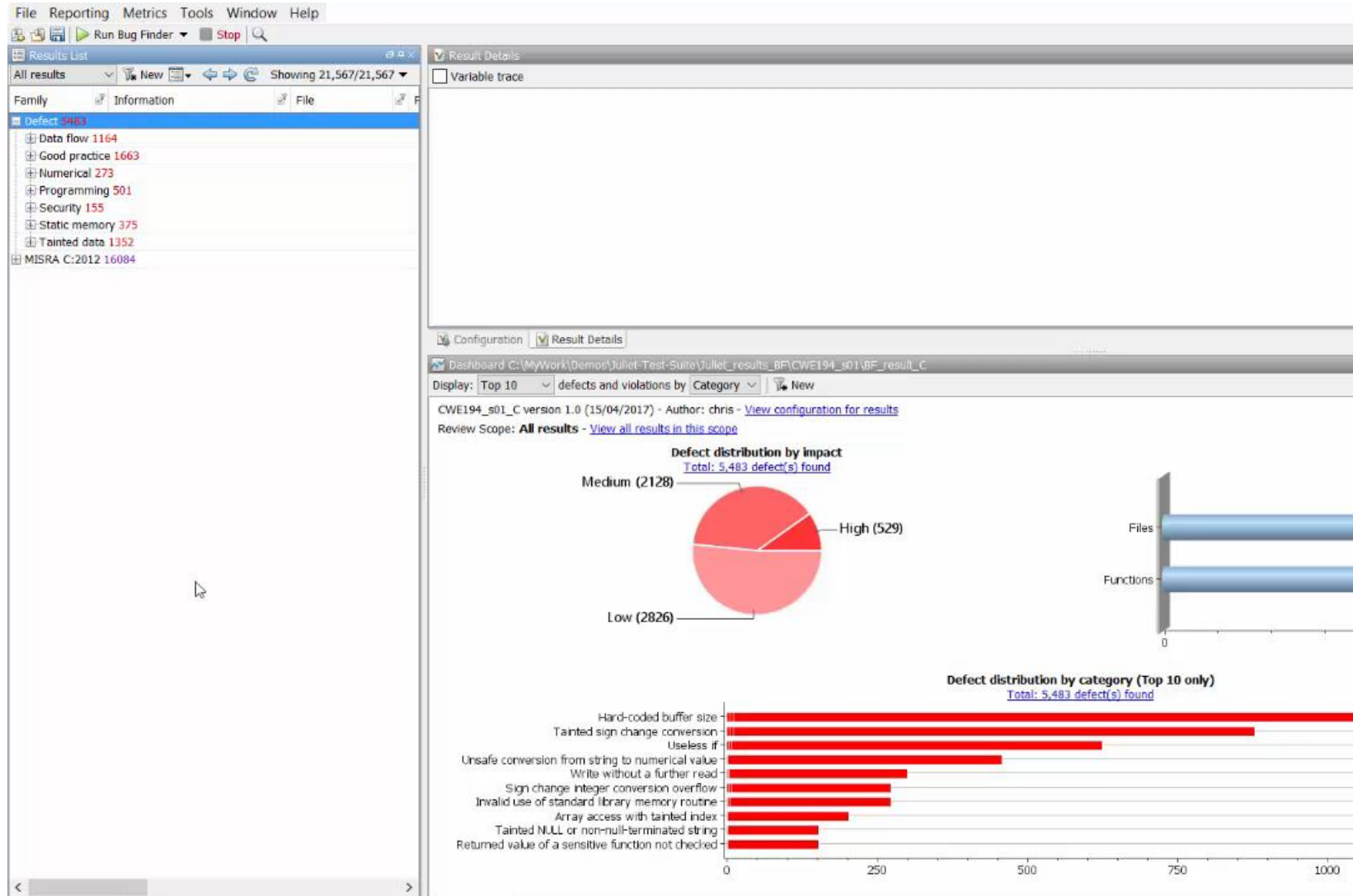
- 不適切な入力確認
- クレデンシャル管理

# Jeepハック – 決定論的乱数発生器 (DRNG)

```
Source
wifi.c x
21
22 char *get_password()
23 {
24     int c_max = 12;
25     int c_min = 8;
26     unsigned int t = time(NULL);
27     srand(t);
28     unsigned int len = (rand()) % (c_max
29     char *password = malloc(len);
30     int v9 = 0;
31     do{
32         unsigned int v10 = rand();
33         int v11 = convert_byte_to_ascii_letter(v10 % 62);
34         password[v9] = v11;
35         v9++;
36     } while (len > v9);
37     return password;
38 }
```



# 「汚染されたデータ」とは？



配列の範囲外アクセス  
(インデックスが負の値)

負の値をインデックス  
に使用

負の値のチェックがない

安全ではないソース  
「汚染されたデータ」  
を読む



# サイバーセキュリティ – 業界活動と標準

## 自動車業界に見られるコーディング標準 & 実践

- **CERT C** : セキュアコーディングスタンダード
- **ISO/IEC TS 17961** : Cセキュアコーディングルール
- **CWE** : 共通脆弱性タイプ
- **MISRA-C:2012** Amendment 1 : 改訂1



## SAE – Vehicle Cybersecurity Systems Engineering Committee

- SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- SAE J3101 - Requirements for Hardware-Protected Security for Ground Vehicle Applications (WIP)
- SAE “Cybersecurity Assurance Testing Task Force” (TEVEES18A1)

# アジェンダ

1. サイバー攻撃の事例紹介

**2. セキュリティ脆弱性の検出**

3. ソフトウェアの安全性の証明

4. ユーザー事例 & まとめ



# Polyspace Bug Finder のスピーディー解析 素早い欠陥検出・修正を可能とする！

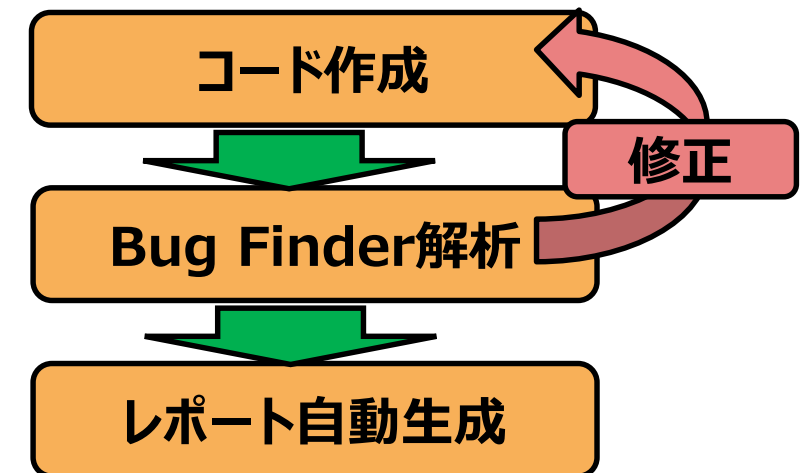
- **セキュリティ脆弱性・バグ検出**
  - コード作成後、すぐに欠陥を検出・修正
- **コーディングルールチェック**
  - エラー予防と再利用性向上
  - MISRA準拠を確認
- **コードメトリックス解析**
  - コードの複雑度を測定

開発プロセスの上流で不具合を発見！  
コードを統合前に多くの欠陥を修正！  
コード開発の効率に繋がる！

```

169
170 extern void useint(int val);
171 void bug_partiallywrittenarray(void)
172 {
173     int tab[5] = { 0, 1, 2, 3, 4 };
174
175     useint(tab[0]);
176     useint(tab[1]);
177     useint(tab[2]);
178     useint(tab[2]); /* Defect: Same index a
179     useint(tab[4]);
180 }
181
182 void com...llywrittenarray(void)
183 {
  
```

時間を掛けずに大部分のバグを識別



# セキュリティ脆弱性・バグ検出項目

## 数値

- ゼロ割、オーバーフロー
- 標準ライブラリ数学ルーチンの無効な使用
- …

## 静的メモリ

- 配列の範囲外アクセス
- NULLポインター
- …

## プログラミング

- 等号演算子による浮動小数点の比較
- 宣言の不一致
- …

## 動的メモリ

- メモリリーク
- 前に解放したポインターの使用
- …

## セキュリティ

- パス操作が脆弱
- 疑似乱数発生器が脆弱
- …

## 汚染されたデータ

- 汚染された文字列形式
- 汚染されたサイズでのメモリの割り当て
- …

## データフロー

- 読取りのない書込み
- 未初期化変数
- …

## 同時実行

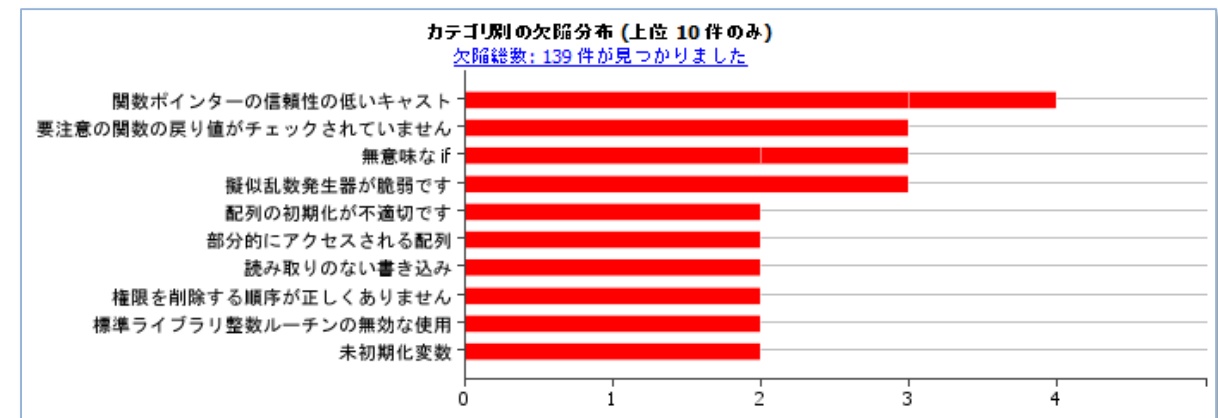
- データレース
- デッドロック
- …

## リソース管理

- 読取り専用リソースに書込み
- 以前に閉じられたリソースを使用
- …

## 適切な手法

- 未使用のパラメータ
- 値渡しの大きな引数
- …





# セキュリティ脆弱性検出サブセット

- **CWE** : 共通脆弱性タイプ
  - CWE™ IDに対応するバグ項目
- **CERT-rules** : セキュアルール
  - CERT Cルールに対応するバグ項目
- **CERT-all** : セキュアルール/推奨
  - CERT Cルール、および、推奨に対応するバグ項目
- **ISO-17961** : Cセキュアコーディングルール
  - ISO/IEC TS 17961コーディング規約  
に対応するバグ項目

脆弱な暗号アルゴリズム (影響: Medium) ?

Encryption algorithm of 'EVP\_EncryptInit\_ex()' does not ensure a sufficient security level. The encrypted data can be retrieved. Use a strong cipher with a strong mode, for example, AES with CBC mode.

イベント	ファイル	スコープ	行
1	Call to EVP_des_cbc	security.c	bug_cryptocipherweakcipher() 1148
2	Assignment to local pointer 'ciph'	security.c	bug_cryptocipherweakcipher() 1148
3	脆弱な暗号アルゴリズム	security.c	bug_cryptocipherweakcipher() 1149

脆弱な暗号アルゴリズム

暗号コンテキストに関連付けられた暗号化アルゴリズムが脆弱

説明

脆弱な暗号アルゴリズムは、暗号コン

リスク

一部の暗号化アルゴリズムには既

するのとは違わなければなりません

暗号アルゴリズムが脆弱な場合、

修正方法

詳しく研究され、安全であると広

たとえば、高度暗号化標準 (AES)

例

> DES アルゴリズムの使

結果情報

グループ: セキュリティ

言語: C | C++

既定値: オフ

コマンドライン構文

「影響」: 中

CWE ID: 325, 326, 327

CWE Webサイト

CWE Common Weakness Enumeration  
A Community-Developed List of Software Weakness Types

CWE-325: Missing Required Cryptographic Step

Weakness ID: 325  
Abstraction: Easy  
Status: Incomplete

Description

Description Summary  
The software does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than advertised by that algorithm.

Extended Description  
Cryptographic implementations should follow the algorithms that define them exactly, otherwise encryption can be weaker than expected.

Applicable Platforms

Languages

All

Common Consequences

Scope: Effect  
Access: Technical Impact: Bypass protection mechanism  
Control: If the cryptographic algorithm is used for authentication and authorization, then an attacker could gain unauthorized access to the system.

Confidentiality: Technical Impact: Read application data; Modify application data  
Integrity: Technical Impact: Modify application data

<https://cwe.mitre.org/data/definitions/325.html?browser=F1help>

ドキュメンテーション & 推奨アクション

# コーディングルールチェック

- **MISRA C® : 2004** チェッカー
- **MISRA C® : 2004 AC AGC** チェッカー
  - 自動生成コード用
- **MISRA C® : 2012** チェッカー
- **MISRA® C++** チェッカー
- **JSF® ++** チェッカー

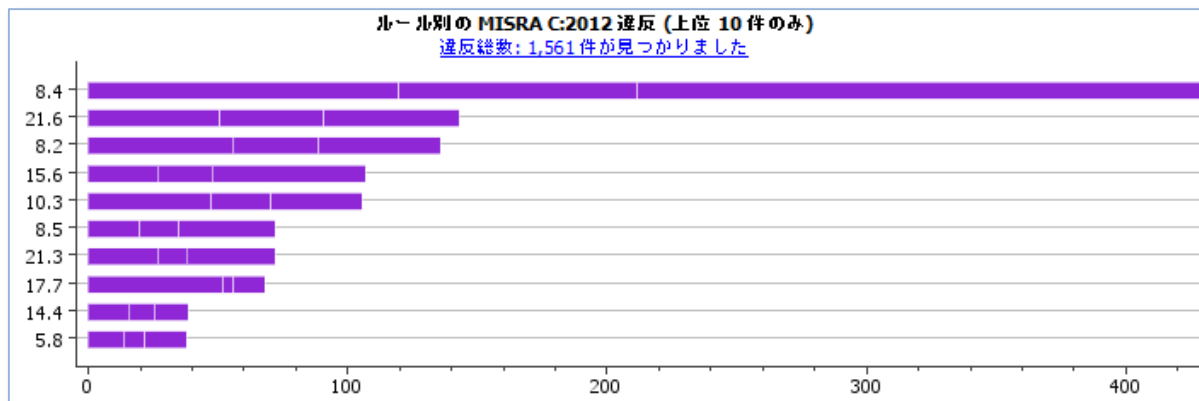


## MISRA C:2012 Amendment 1

Additional security  
guidelines for MISRA C:2012

April 2016

- ✓ **新しいコーディング規約** に対応  
(全ての required と mandatory)
- ✓ **新しい指針 (directive) : 1**
- ✓ **新しいルール (rules) : 13**
- ✓ 既存のルール変更 [21.8]



## MISRA-C:2012 改訂1 の新しい指針4.14の例

```
int corrected_taintedintdivision(int usernum, int userden) {
    int r = 0;

    if (userden!=0 && !(usernum=INT_MIN && userden==-1)) {
        r = usernum/userden;
    }

    print_int(r);
    return r;
}
```

汚染されたデータによる除算

○\* Tainted division operand (Impact: Low)

▽\* MISRA C:2012 D4.14 (Required)

▽ MISRA C:2012 D4.14 (Required) ?

The validity of values received from external sources shall be checked. Division (/) operation operands are from an unsecure source. Check for:

- Denominator of zero.
- Numerator of minimum value and denominator of -1.

# アジェンダ

1. サイバー攻撃の事例紹介
2. セキュリティ脆弱性の検出
- 3. ソフトウェアの安全性の証明**
4. ユーザー事例 & まとめ



# バグを見つけることができますか？

```
ソース
検索結果の統計 WhereAreTheErrors.c
1 int new_position(int sensor_pos1, int sensor_pos2)
2 {
3     int actuator_position;
4     int x, y, tmp, magnitude;
5
6     actuator_position = 2; /* default*/
7     tmp = 0; /* values */
8     magnitude = sensor_pos1 / 100;
9     y = magnitude + 5;
10
11     while (actuator_position < 10)
12     {
13         actuator_position++;
14         tmp += sensor_pos2 / 100;
15         y += 3;
16     }
17     if ((3*magnitude + 100) > 43)
18     {
19         magnitude++;
20         x = actuator_position;
21         actuator_position = x / (x - y);
22     }
23     return actuator_position*magnitude; /* value */
24 }
```

未初期化の可能性

オーバーフローの可能性

ゼロ割の可能性

**actuator\_position = x / (x - y);**

# Polyspace Code Prover の実行結果

```
ソース
検索結果の統計 WhereAreTheErrors.c
1 int new_position(int sensor_pos1, int sensor_pos2)
2 {
3 int actuator_position;
4 int x, y, tmp, magnitude;
5
6 actuator_position = 2; /* default*/
7 tmp = 0; /* values */
8 magnitude = sensor_pos1 / 100;
9 y = magnitude + 5;
10
11 while (actuator_position < 10)
12 {
13     actuator_position++;
14     tmp += sensor_pos2 / 100;
15     y += 3;
16 }
17 if ((3*magnitude + 100) > 43)
18 {
19     magnitude++;
20     x = actuator_position;
21     actuator_position = x / (x - y);
22 }
23 return actuator_position*magnit
24 }
```

operator / on type int 32  
left: 10  
right: [-21474855 ... -1]  
result: [-10 .. 0]

- ✓ あらゆる条件でコードの安全性を証明
- ✓ テストを行わずに網羅的に解析
  - 実行時エラー
  - 条件による実行時エラー
  - 到達不能なコード

**actuator\_position = x / (x - y);**



# Polyspace Code Prover でコードの正しさを証明 全ての実行パスの結果を証明する！

- Quality (品質)
  - ランタイムエラーの証明
  - 測定、向上、管理
- Usage (使用方法)
  - コンパイル、プログラム実行、テストケースは不要
  - 対応言語：C/C++/Ada
- Process (プロセス)
  - ランタイムエラーの早期検出
  - 自動生成コード、ハンドコードの解析可能
  - コードの信頼性を測定

実機実験前にコード信頼性を  
確保して手戻りを削減

**グリーン：正常**  
ランタイムエラーが存在しない

**レッド：エラー**  
実行される度にランタイムエラー

**グレー：デッドコード**  
無実行

**オレンジ：Unproven**  
条件によってランタイムエラー

**パープル：Violation**  
MISRA-C/C++, JSF++

変数値範囲  
ツールチップ

```
static void pointer_arithmetic (void) {
    int array[100];
    int *p = array;
    int i;

    for (i = 0; i < 100; i++) {
        *p = 0;
        p++;
    }

    if (get_bus_status() > 0) {
        if (get_oil_pressure() > 0) {
            *p = 5;
        } else {
            i++;
        }
    }

    i = get_bu

    if (i >= 0) {
        *(p - i) = 10;
    }
}
```

Dereference of local pointer 'p'  
(pointer to int 32, size: 32bits):  
Points to 4 bytes at offset 400 in  
buffer of 400 bytes, so is outside  
bounds.

# Polyspace Code Prover – ソフトウェアの安全性の確保

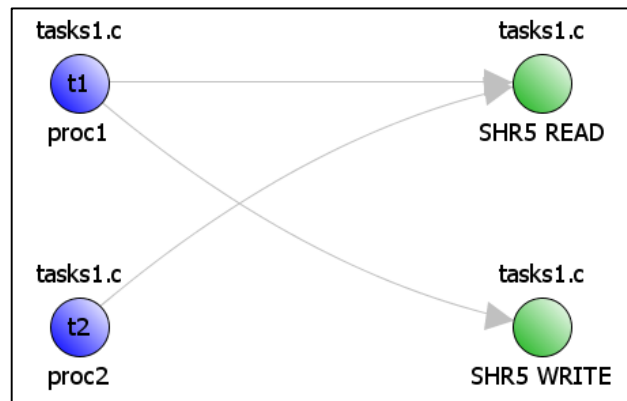
- MISRAルール違反の安全性の証明



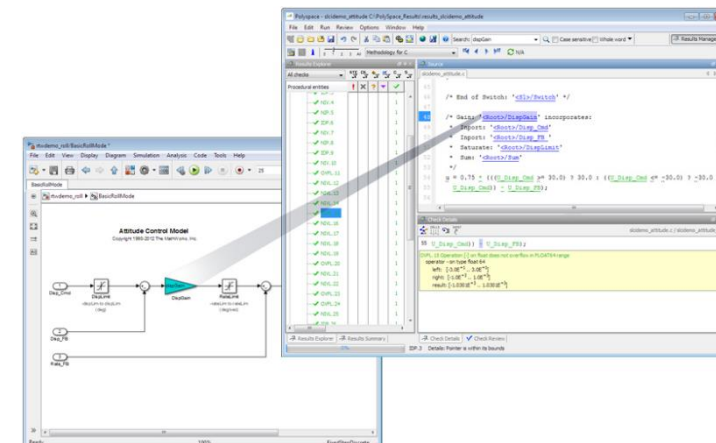
- 機能安全規格に準拠



- グローバル変数の同時アクセスの特定



- MBDとの統合による安全性の確保



# MISRAルール違反の安全性の証明

```
13 float risk_of_floatdivisionbyzero(int p)
```

**MISRA  
ルール違反**

**安全性の証明  
(オーバーフロー無し)**

Check Details

Misra\_C2004.c / risk\_of\_floatdivisionby

**ID 7: MISRA C:2004 10.1**  
The value of an expression of integer type shall not be implicitly converted to a different underlying type.  
Implicit conversion of the binary - right hand operand of underlying type 'signed int' to 'float' that is not an integer type. (Required)

**✓ ID 130: Overflow**  
Operation [-] on float does not overflow in FLOAT32 range  
operator - on type float 32  
left: 1.0  
right: [-2.1475E+09 .. -0.9999] or [0.0 .. 2.1475E+09]  
result: [-2.1475E+09 .. 2.1475E+09]

Check Review

**MISRA C:2004 10.1**

Classification  
Not a defect

Status  
No action planned

Justified

proven correct

**Polyspace Code Prover**

**MISRAルール違反の正当化の  
根拠としてPolyspaceを活用可能**

```
24     } else {
25         i = 0.0;
26     }
27     return i;
28 }
```

# グローバル変数の同時アクセスの特定

## マルチタスク時のレビューを効率化

```
tasks1.c X
29 static int SHR5 = 5;
```

### 対話的なレビュー手法

保護された変数

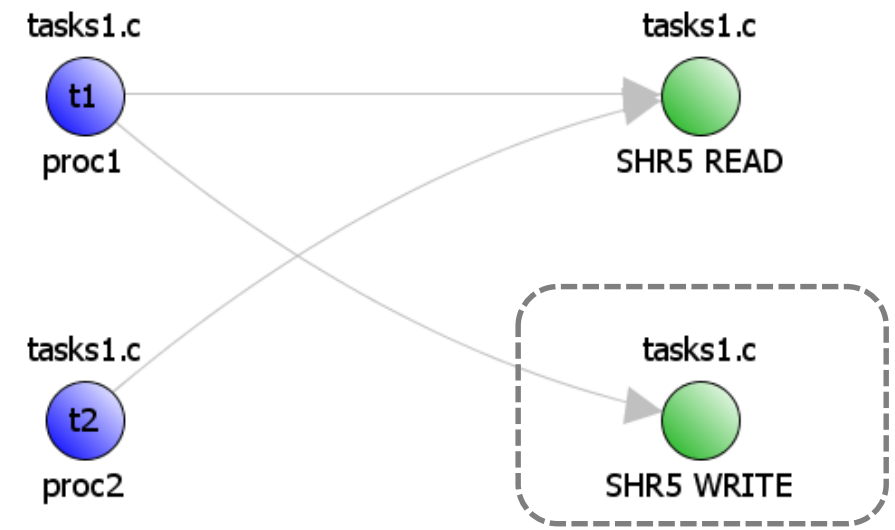
Variable 'tasks1.SHR5' is shared among several tasks.

読み取り元タスク: [proc1](#) [proc2](#)

書き込み元タスク: [proc1](#)

	イベント	ファイル	スコープ	行
◀	書き込み値: 5	tasks1.c	<u>_init_globals()</u>	29
◀	書き込み値: 28	tasks1.c	proc1()	103
▶	読み取り値: 5	tasks1.c	proc1()	103
▶	読み取り値: 5 or 28	tasks1.c	proc2()	112

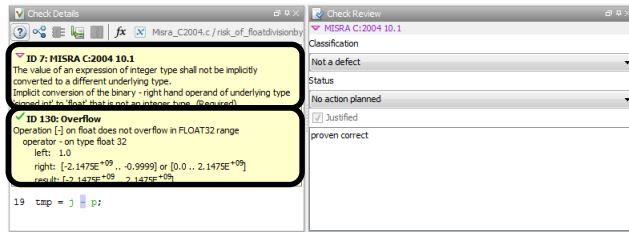
### グラフィカルなレビュー手法



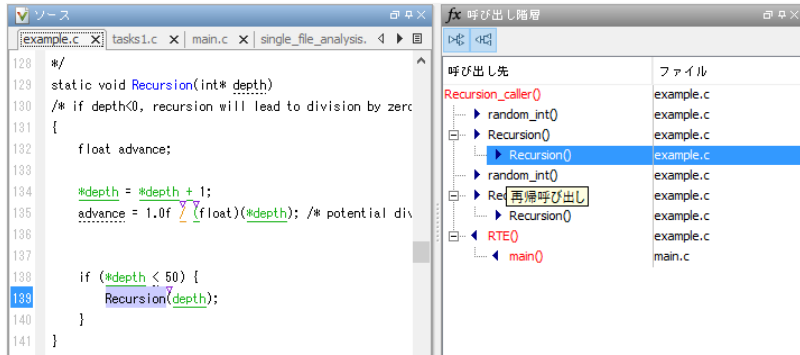
- グリーン** : 同時アクセスから保護
- グレー** : 定義しているが未使用
- オレンジ** : 競合の可能性あり



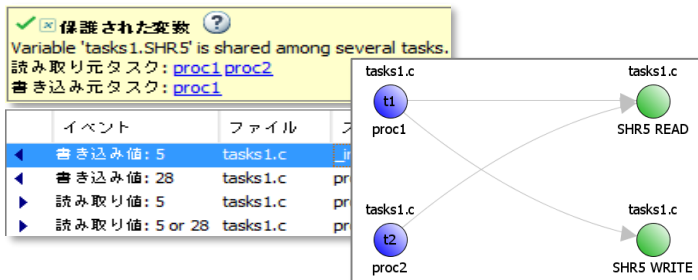
# Polyspace Code Prover – ISO26262適用



## MISRAルール違反の安全性の証明



## 再帰呼び出しの識別



## グローバル変数の同時アクセスの特定

Table 8 – Design principles for software unit design and implementation **ソフトウェアユニット設計と実装の基本原則**

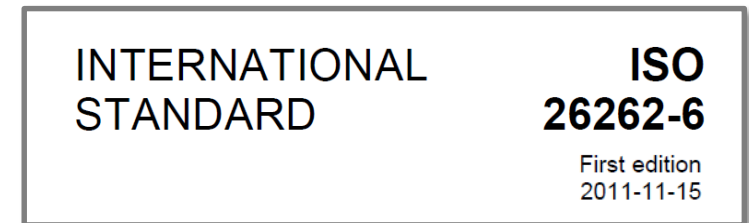
Methods		ASIL (安全性要求レベル)			
		A(低)	B	C	D(高)
1g	No implicit type conversions <b>暗黙の型変換の禁止</b>	+	++	++	++
1j	No recursions <b>再帰呼び出しの禁止</b>	+	+	++	++

++ : 強く推奨、+ : 推奨

Table 9 – Methods for the verification of software unit design and implementation **ソフトウェアユニット設計の検証方法**

Methods		ASIL (安全性要求レベル)			
		A(低)	B	C	D(高)
1g	Data flow analysis <b>データフロー解析</b>	+	+	++	++

++ : 強く推奨、+ : 推奨



# 規格準拠に向けて Polyspace製品で目標規格達成をアシストします！

- コーディング規約
  - MISRA-C
  - MISRA-C++
  - JSF++
- ソフトウェアメトリクス
  - HIS Source Code Metrics
    - <http://www.automotive-his.de/>
- 認証規格
  - DO-178B
    - DO Qualification Kit
  - IEC 61508, ISO 26262, EN 50128
    - IEC Certification Kit

CERTIFICADO ◆ CERTIFICAT



## CERTIFICATE

No. Z10 09 07 67052 003

<b>Holder of Certificate:</b>	<b>The MathWorks, Inc.</b> 3 Apple Hill Drive Natick MA 01760-2098 USA
<b>Factory(ies):</b>	63726
<b>Certification Mark:</b>	
<b>Product:</b>	<b>Software Tool for Safety Related Development</b>
<b>Model(s):</b>	<b>PolySpace® Client™ for C/C++ PolySpace® Server™ for C/C++</b>
<b>Parameters:</b>	The verification tools are fit for purpose to verify safety related software according to IEC 61508, EN 50128, ISO 26262, and derivative standards. The verification tools are qualified tools according to ISO 26262. The report MN74651C is a mandatory part of this certificate.

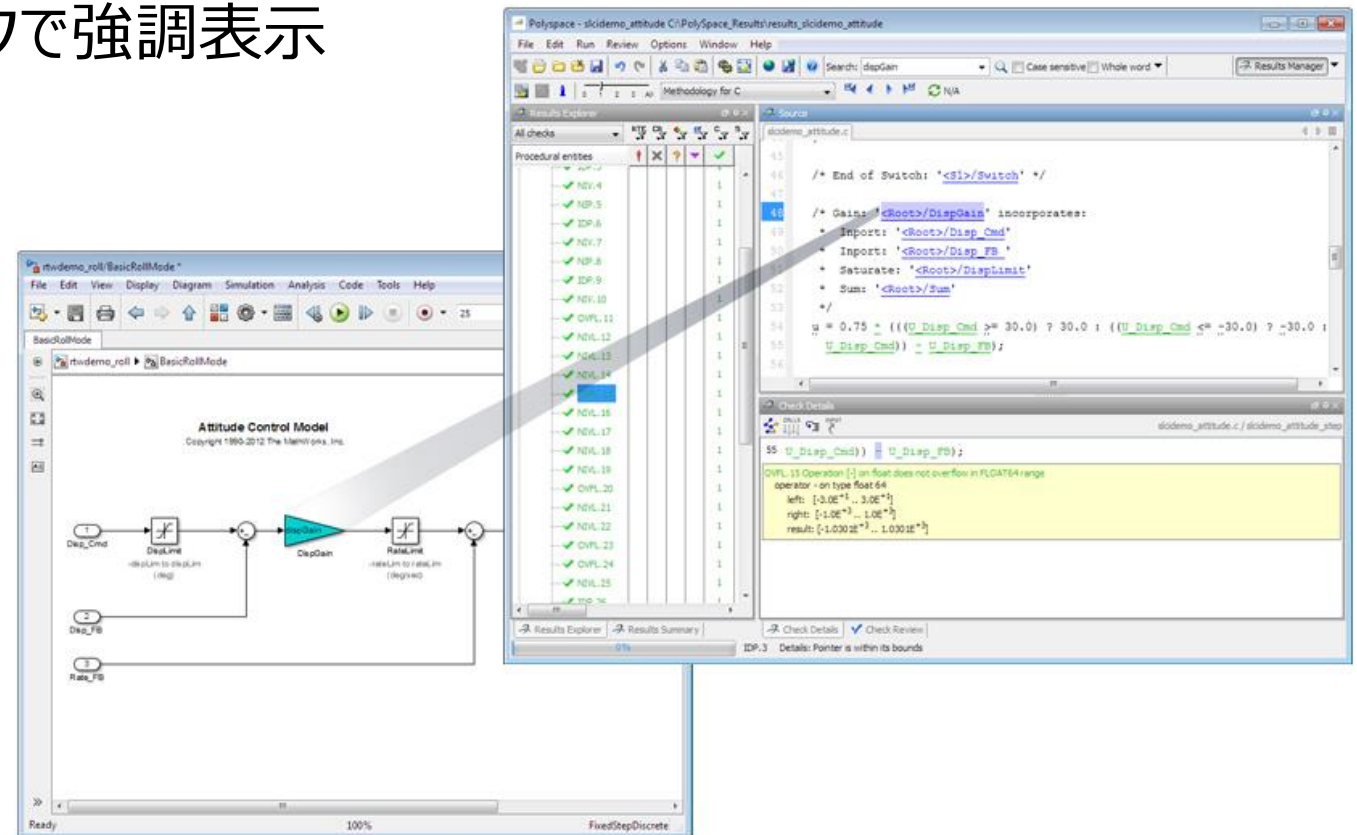
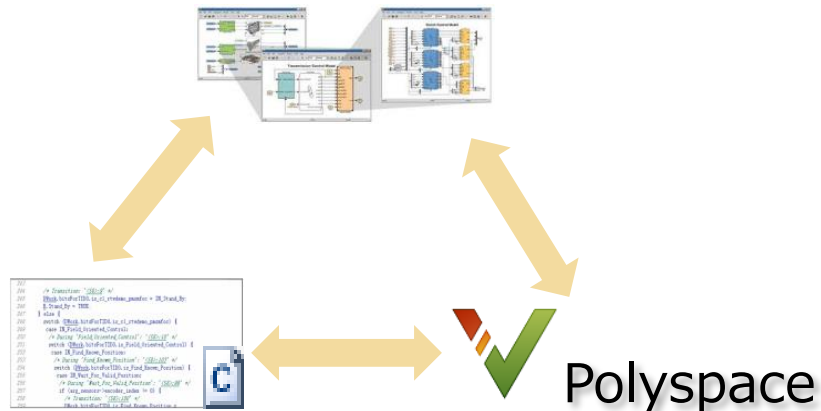
CERTIFICADO ◆ CERTIFICAT

認証書

# モデルベースデザインとの統合

## PolyspaceのSimulink連携機能でモデル修正が容易

- Simulink®環境からPolyspace解析を実行
- Polyspace解析結果を該当ブロックで強調表示
- ブロックにPolyspaceの注釈を追加
- S-Functionコードの検証
- MISRA C のチェック



# アジェンダ

1. サイバー攻撃の事例紹介
2. セキュリティ脆弱性の検出
3. ソフトウェアの安全性の証明
- 4. ユーザー事例 & まとめ**

# Polyspace ユーザー事例

## 医療、航空、自動車など様々な分野で利用されています

### Miracor Eliminates Run-Time Errors and Reduces Testing Time for Class III Medical Device Software



“From a developer’s perspective, the main advantage of Polyspace Code Prover is a higher level of quality and correctness in the code. Polyspace Code Prover helps Miracor demonstrate this quality and correctness to the regulatory community, including the FDA, to prove that our device is safe.”

- Lars Schiemanck, Miracor Medical Systems

[https://jp.mathworks.com/company/user\\_stories/miracor-eliminates-run-time-errors-and-reduces-testing-time-for-class-iii-medical-device-software.html](https://jp.mathworks.com/company/user_stories/miracor-eliminates-run-time-errors-and-reduces-testing-time-for-class-iii-medical-device-software.html)

### Solar Impulse Develops Advanced Solar-Powered Airplane



“From a developer’s perspective, the main advantage of Polyspace Code Prover is a higher level of quality and correctness in the code. Polyspace Code Prover helps Miracor demonstrate this quality and correctness to the regulatory community, including the FDA, to prove that our device is safe.”

- Lars Schiemanck, Miracor Medical Systems

[https://jp.mathworks.com/company/user\\_stories/solar-impulse-develops-advanced-solar-powered-airplane.html](https://jp.mathworks.com/company/user_stories/solar-impulse-develops-advanced-solar-powered-airplane.html)

### 日産自動車 ソフトウェアの信頼性を向上

「Polyspace 製品によって、高レベルなソフトウェアの信頼性を確保することができます。これは、業界内の他のツールにはできないことです。」

- 菊池光彦氏, 日産自動車



#### 課題

ソフトウェア品質を向上させるために、発見が困難なランタイムエラーを特定する

#### ソリューション

MathWorks のPolyspace製品を使用して、日産とサプライヤーのコードを包括的に解析する

#### 結果

サプライヤーのバグを検出して評価  
ソフトウェアの信頼性が向上  
日産のサプライヤーが Polyspace 製品を採用

[https://jp.mathworks.com/company/user\\_stories/nissan-increases-software-reliability.html](https://jp.mathworks.com/company/user_stories/nissan-increases-software-reliability.html)



## Polyspace – まとめ

### 静的解析によるコード検証でセキュリティと安全性の確保

#### Polyspace Bug Finder™ によるセキュリティ脆弱性の検出

- ✓ セキュリティ脆弱性とバグの早期検出
- ✓ コーディングルールのチェック
- ✓ セキュリティ項目のドキュメンテーション  
& 推奨アクション

#### Polyspace Code Prover™ による安全性の証明

- ✓ あらゆる条件でコードの安全性を証明
- ✓ ソフトウェアの安全性の確保
  - MISRAルール違反の安全性の証明
  - グローバル変数の同時アクセスの特定
  - 機能安全規格のツール認証に対応
  - MBDとの統合による安全性の確保





## Polyspace – まとめ

静的解析によるコード検証でセキュリティと安全性の確保

Polyspace Bug Finder™  
によるセキュリティ脆弱性の検出

Polyspace Code Prover™  
による安全性の証明

セキュリティと安全性の確保で

ソフトウェアの品質を向上する

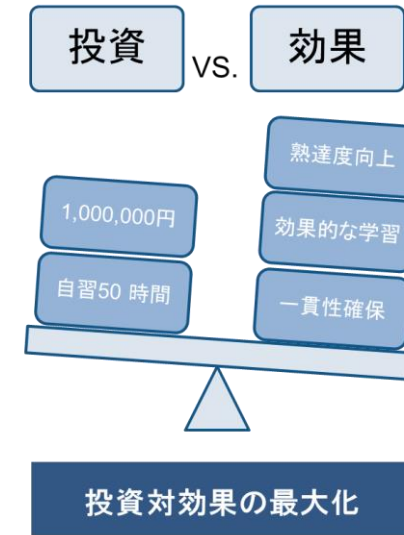
Polyspace 静的解析ソリューション

- MBDとの統合による安全性の確保
- 機能安全規格のツール認証に対応

# Polyspace の有効活用に向けて 短期間で習得していただけるような教育カリキュラムをご提供します

## Polyspace Bug Finder による C/C++コードの解析 新

この1日コースでは、Polyspace Bug Finder™ 製品を使用して、コーディングの欠陥やソフトウェアの品質メトリックの改善、製品の完全性について学びます。組み込みシステム向けのソフトウェアやモデルの開発をご担当される技術者を対象とした実践的な内容になっています。



## Polyspace Code Prover による C/C++コードの検証

この2日コースでは、Polyspace Bug Finder および Polyspace Code Prover™ 製品を使用して、コードの正確性やソフトウェアの品質メトリックの改善、製品の完全性について学びます。

# ご清聴ありがとうございました



Accelerating the pace of engineering and science

© 2017 The MathWorks, Inc. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See [www.mathworks.com/trademarks](http://www.mathworks.com/trademarks) for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.