2018年12月4日

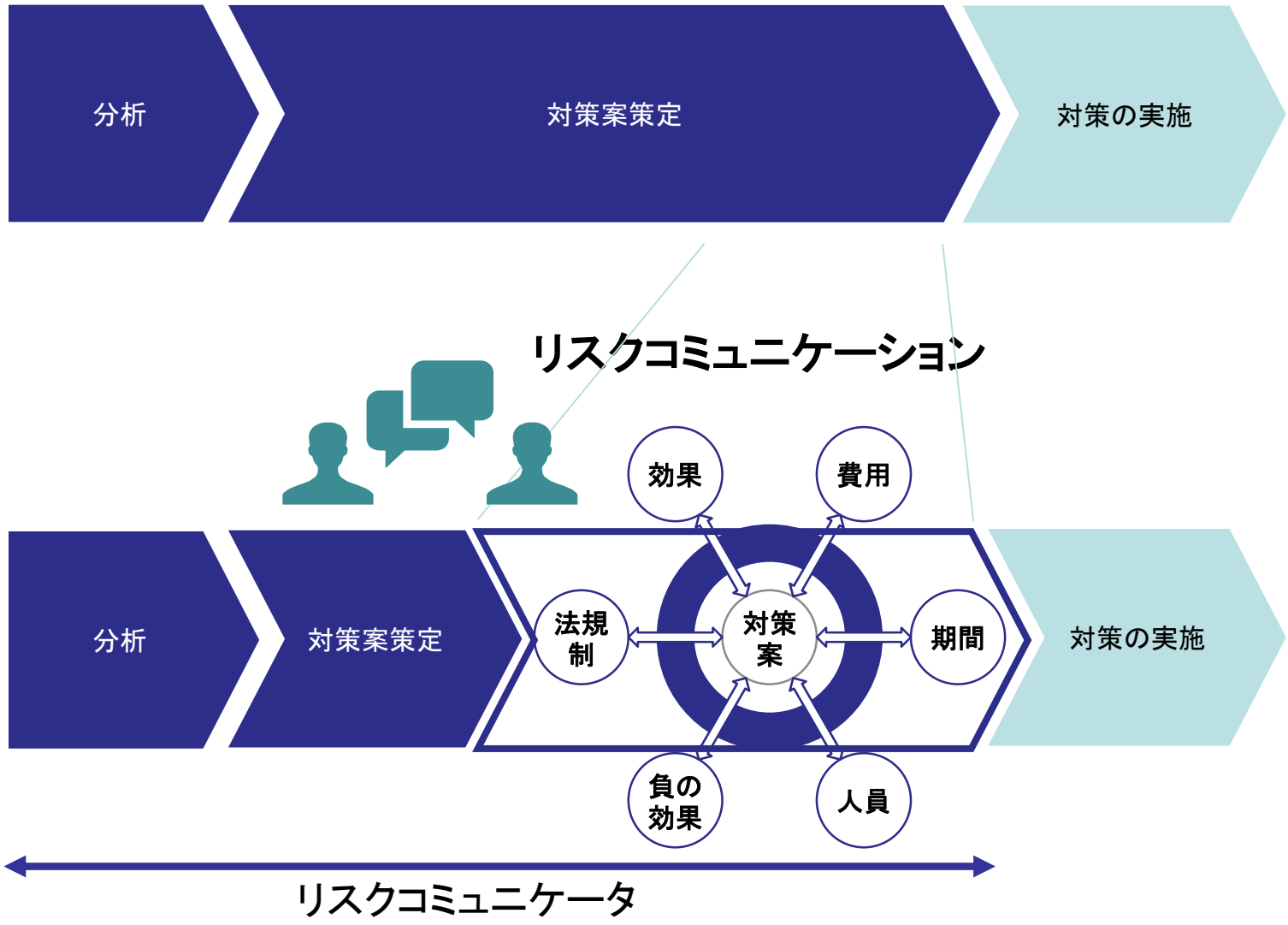
# IoT向けリスクコミュニケーション支援ツールMRC4IoTの開発と試適用

東京電機大学総合研究所
林　浩史
高橋　雄志*
金子　朋子
佐々木良一

# Agenda

1. はじめに(リスクコミュニケーションとは）
2. 多重リスクコミュニケータ（MRC）の開発経緯
3. IoT向けリスクコミュニケーションの流れ
4. SafetyとSecurityの同時分析
5. IPA STAMP Workbenchの活用
6. MRC4IoTの紹介
7. まとめ

# リスクコミュニケーションとは



# 多重リスクコミュニケータ（MRC）の開発

＜背景＞

背景1．多くのリスク（セキュリティリスク、プライバシーリスクなど）が存在＝＞リスク間の対立を回避する手段が必要

背景2．ひとつの対策だけでは目的の達成が困難＝＞対策の最適な組み合わせを求めるシステムが必要

背景3．多くの関与者（経営者・顧客・従業員など）が存在＝＞多くの関与者間の合意が得られるコミュニケーション手段が必要

MRCにおける対応

①多くのリスクやコストを考慮しつつ望ましい対策組み合わせを求める問題として定式化

②関与者の合意が得られるまで条件別の望ましい対策案の算出を実施

専門家

対策案
①②③④

定式化結果

多重リスクコミュニケータMRC

**最適解**
対策案
①③の組合せ

満足

Y

END

N

制約条件などの変更

ファシリテータ　関与者

佐々木良一「ITリスク学の提案と最近の動向」情報処理学会論文誌、Vol.55,No.9,pp1946-1955（2014年）

# MRCの適用

①適用対象
（a）個人情報漏洩対策（含む：世田谷区役所の個人情報漏洩対策への実適用など）
（b）内部統制問題など
＝＞参加者が5-6人までなら基本的有効性を確認

②受賞
（a）日本セキュリティ・マネジメント学会2009年度論文賞受賞
（b）情報処理学会DICOMO2010最優秀論文賞受賞
（c） IEEEのCFSE2012での招待講演

詳しくは佐々木良一他「多重リスクコミュニケータの開発と適用」
情報処理学会論文誌、Vol49,No9、2008年9月号

# MRCについて機能の拡張

（1）標的型攻撃等多段にわたる攻撃のリスク評価のためのリスク解析法（EDC法）の開発

（2）被害発生防止対策と復元対策の両方を考慮した対策案最適組合せ法（InfoSec2014 Best Paper Award受賞）

（3）動的リスクを考慮した多重リスクコミュニケータ

（4）経営者とのリスクコミュニケーションも考慮した多重リスクコミュニケータ

（5）合意形成対象者が1000人を超すような問題への適用
　Social-MRCを開発し、青少年への情報フィルタリング問題への適用（情報処理学会DICOMO2010　最優秀論文賞など)

（6）IoTシステム向けのリスクコミュニケータ（MRC4IoT）

# IoT機器に適用できるように
# リスクコミュニケーション手法の拡張

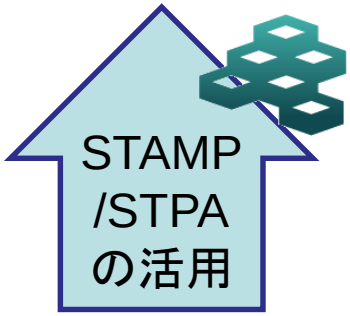
① IoT機器システムは制御系を含み、従来のアタックツリーのようなものだけではセーフティの評価が困難 ＝＞
MITのナンシーレブゾン提案のSTAMP/STPA手法（セキュリティは対象外）を改良して使用

② セキュリティ、セーフティ、メインテナビリティなど異なる指標を扱う必要がある ＝＞
（a） リスクベースの統一的指標を採用
（b） 原因となる故障やヒューマンエラーだけでなくサイバー攻撃によるものも統一的に記述できる**ガイドテンプレイトの提案**

③ リスクを評価するためにはいろいろなアプローチがあり、一長一短がある ＝＞
（a） 定量的アプローチと準定量的アプローチの統合
（b） ボトムアップアプローチとトップダウンアプローチの統合

# IoT向けリスクコミュニケーションの流れ

- [脅威抽出] リスク分析を行いシステムのリスクを抽出
  STAMP/STPAを活用
- STAMP/STPAにより抽出された、脅威を準定量評価
- 対策案の策定
- 対策案実施により期待される効果の準定量評価
- 実施対策案の費用対効果の算出

# SafetyとSecurityの同時分析

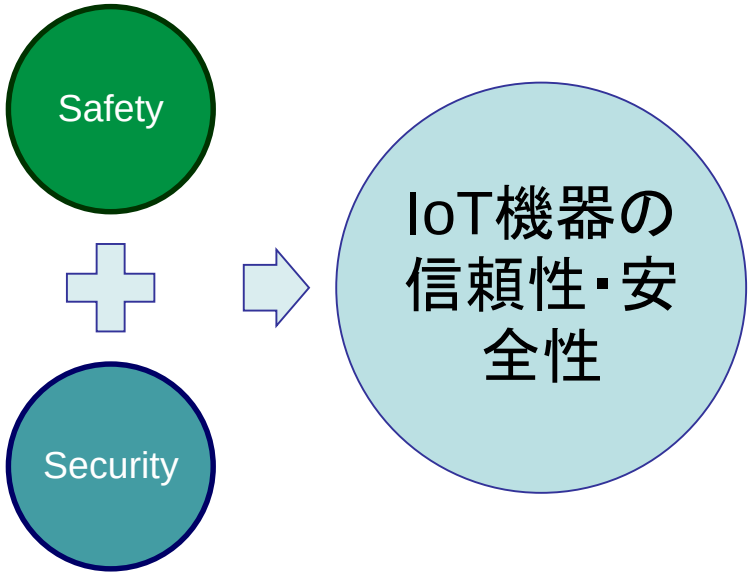
IoT機器

組み込み機器　＋　通信機能

信頼性・安全性　：　Safetyと　Securityの同時実現が必要

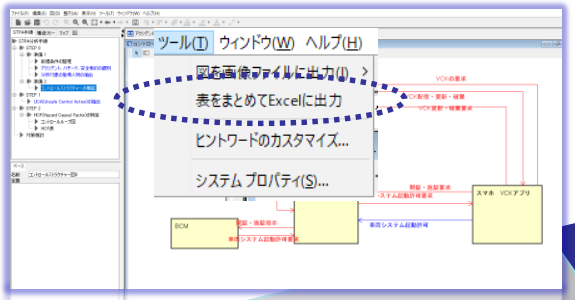
STAMP STPAを用いた分析

ヒントワードの工夫などにより、
SafetyとSecurityの
両方の脅威を同時に
取り扱うことが可能

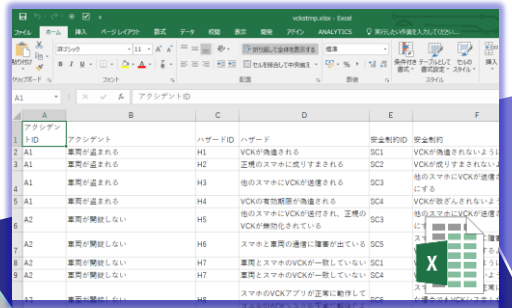



ここでは　Safety, Securityを以下のように定義しています
Safety:実装した機能が期待どおりに動作する状態を維持すること
Security:サイバー攻撃などの脅威に対する体制や対策により、
期待した動作する状態を維持または想定していない動作を行わないようにすること

# STAMP/STPA Workbenchの活用




STAMP/STPA分析を実施



表をまとめてExcelに出力

MRC4IoTに読み込んで準定量分析

STAMP Workbench

MRC4IoT

# IoT向けリスクコミュニケーション支援ツールMRC4IoTの開発

- 機能概要
  - STAMP Workbenchから分析結果を取り込む
  - リスク指向分析による準定量解析
    - 各アクシデント・インシデントの影響を準定量化
    - 各HCFや脅威の準定量化とFault・Attack Treeの構築
    - 各アクシデント・インシデントのリスクレベルの算出
  - 対策案の作成補助
  - 対策毎の費用対効果算出および予算内で実施した場合の想定効果算出

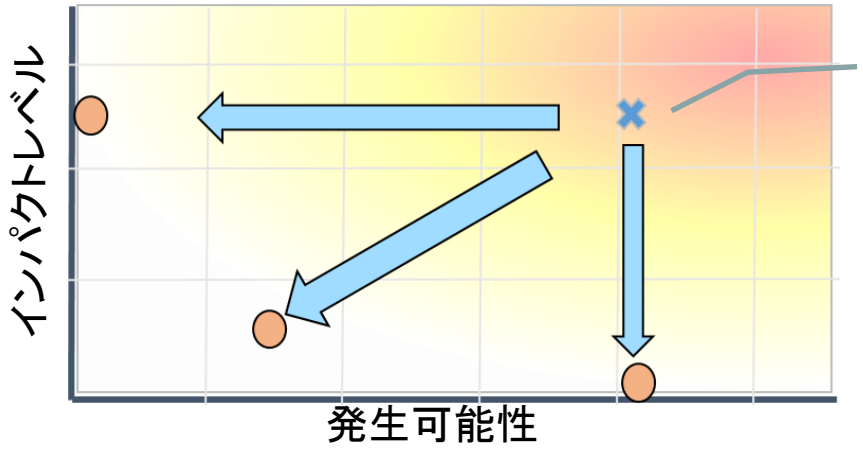
- 開発言語
  - VBA (エクセルマクロ） - Excel 2016(Windows版）上で動作確認

- 規模などを書く
  - 約7K steps程度

# リスク指向分析の考え方

- 準定量分析として、リスク指向分析を採用
- リスク指向分析とは

リスク ＝ アクシデント・インシデントが起きた時のインパクト × アクシデント・インシデントの発生頻度




あるインシデントのリスク

- アクシデント・インシデントが起きた時の「インパクト」と「発生頻度」をそれぞれ分析

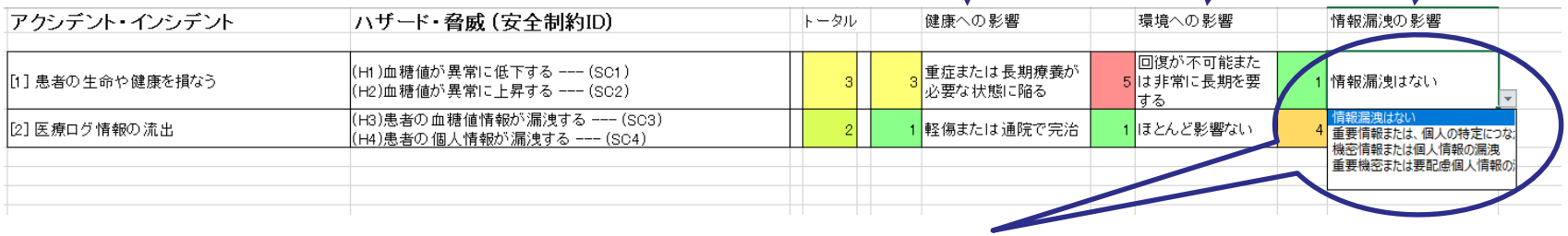
# アクシデント・インシデントが起きた時のインパクトの考え方

- 守るべきもの（Asset)の持つ価値から算出
- 「何を守りたいのか」 を検討する必要

MRC4IoTでは

- 健康への影響
- 環境への影響
- 情報漏洩の影響

を軸としました



| アクシデント・インシデント | ハザード・脅威（安全制約ID) | トータル | | 健康への影響 | | 環境への影響 | | 情報漏洩の影響 |
|---|---|---|---|---|---|---|---|---|
| [1] 患者の生命や健康を損なう | (H1)血糖値が異常に低下する ---（SC1）<br>(H2)血糖値が異常に上昇する ---（SC2） | 3 | 3 | 重症または長期療養が必要な状態に陥る | 5 | 回復が不可能または非常に長期を要する | 1 | 情報漏洩はない |
| [2] 医療ログ情報の流出 | (H3)患者の血糖値情報が漏洩する ---（SC3）<br>(H4)患者の個人情報が漏洩する ---（SC4） | 2 | 1 | 軽傷または通院で完治 | 1 | ほとんど影響ない | 4 | 情報漏洩はない<br>重要情報または、個人の特定につな<br>機密情報または個人情報の漏洩<br>重要機密または要配慮個人情報の |

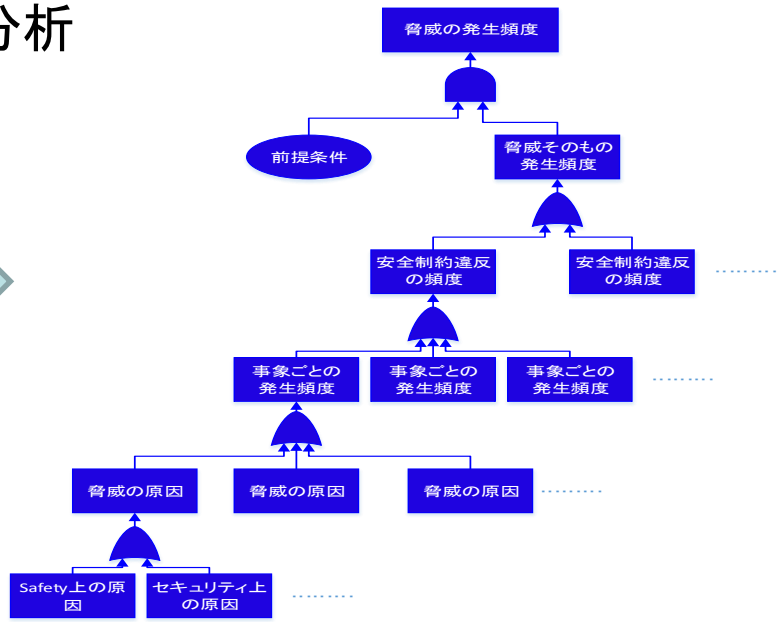
各軸について、5段階の準定量表現で入力

入力は言葉による　選択肢で選ぶものとし、入力者による違いをできる限り排除

# アクシデント・インシデントの発生頻度の考え方

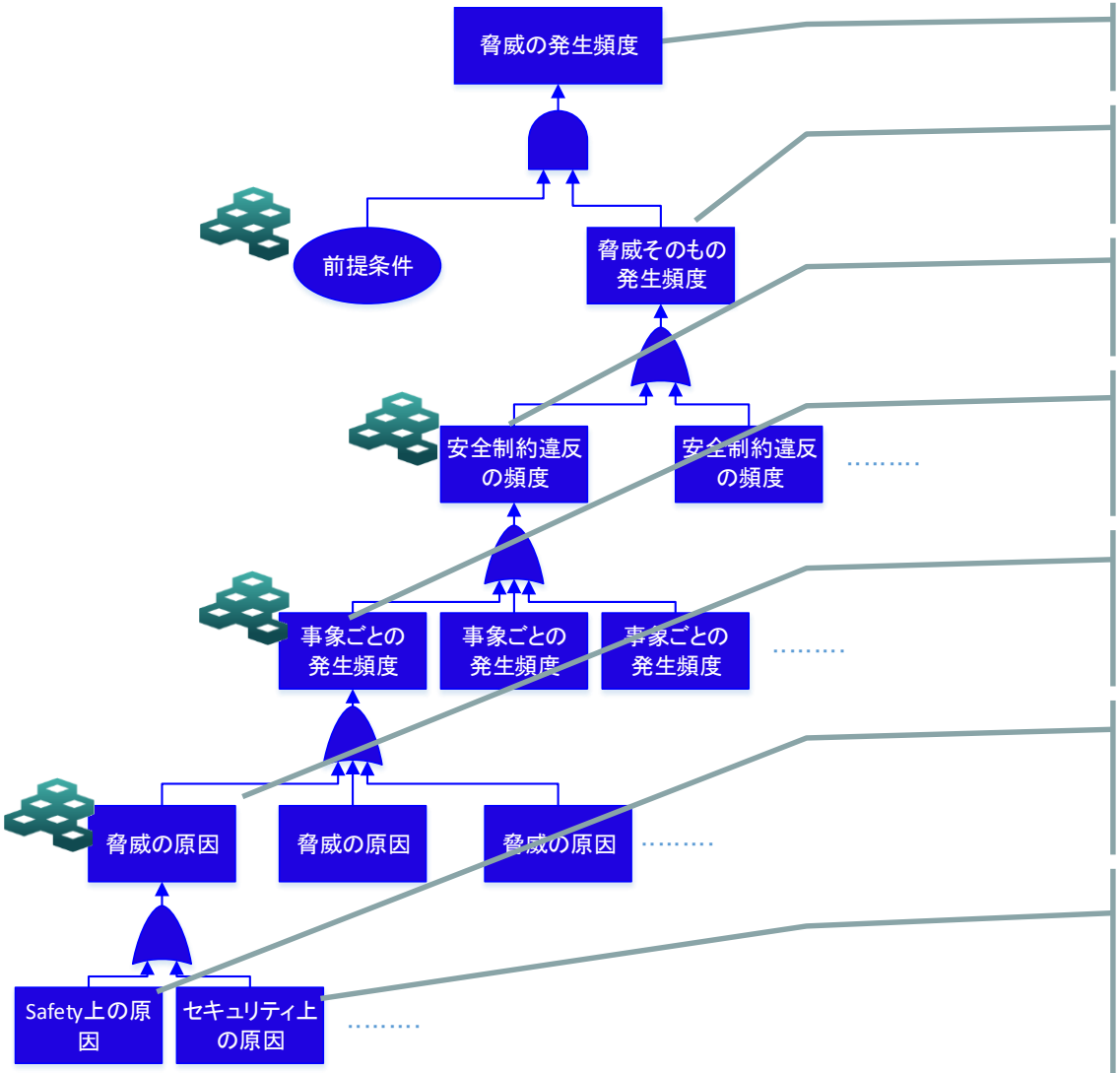
- 脅威やハザードの特徴から準定量化
- STAMP/STPAを用いて脅威を抽出
- ハザードは、発生頻度（例えば部品の　MTBF※など）を利用
- 脅威は、脅威実施に悪用されると想定される
  脆弱性のCVSS※を利用してモデル化
- 全体をFault・Attack Treeとして準定量分析

STAMP Workbench




※MTBF：　Mean Time Between Failure - 平均故障間隔
※CVSS：　Common Vulnerability Scoring System - 共通脆弱性評価システム

# STAMP/STPAを用いた脅威の発生可能性の算出




脅威の発生可能性（頻度）

前提条件を考慮する前の脅威の発生可能性（頻度）

**安全制約**違反の発生可能性（頻度）

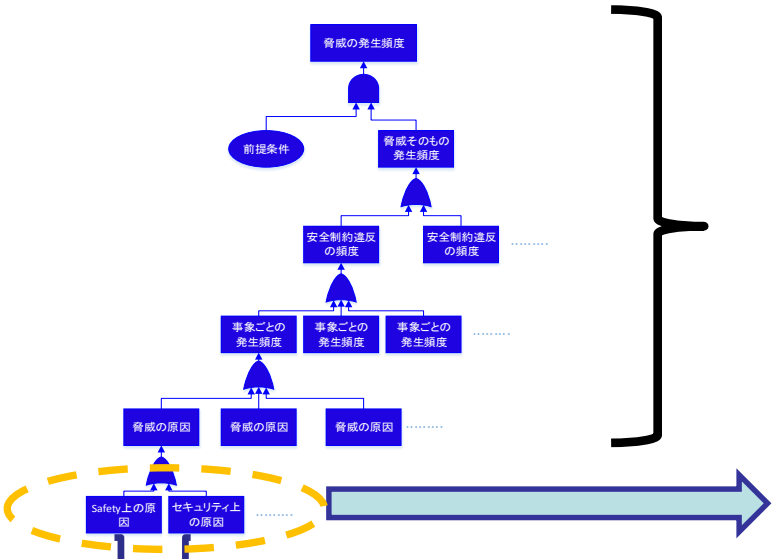
事象（**UCA、 UnSecure Action**）の発生可能性（頻度）

脅威の原因（**HCF, Threat Cause Factor**）の発生可能性（頻度）

脅威の原因の構成要素
ハザードに起因する原因
（MTBFなどの活用）

脅威の原因の構成要素
セキュリティ上の原因
CVSS基本評価基準を活用

# MRC4IoTを用いたリスク分析




- MRC4IoTが、STAMP/STPA Workbenchのエクセル出力を読み込んで自動生成
- 各脅威原因（HCF/Threat Cause Factor）について、セーフレベル・セキュリティレベルを選択

| 脅威の原因 | | セーフレベル | | セキュリティレベル | | 攻撃元区分(AV) | 攻撃条件の複雑さ(AC) | 必要な特権レベル(PR) | ユーザー関与レベル(UI) |
|---|---|---|---|---|---|---|---|---|---|
| 1.62E-02 | 電源喪失 [(1) EN:環境要因] | | | 1.62E-02 | 0.82 | ネットワーク | 高 | 不要 | 不要 |
| 4.24E-02 | センサー故障 [(2)FA:機器故障] | 3.65E-02 | 起こり得るが稀 MTBF 1,000時間程度をイメージ | 3.17E-03 | 0.00 | | | | |
| 1.10E-02 | センサープログラムのバグ [(3)BG:プログラムのバグ] | | | 1.10E-02 | 0.39 | ローカル | | 低 | 要 |
| 3.69E-01 | 患者が人体からセンサーを取り外す [(4)HE:ヒューマンエラー] | 3.65E-01 | 頻繁に起こることが前提 MTBF 100時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 1.69E-02 | マルウエアによるセンサーAPプログラムや出力値の改ざん [(6)Tamper:改ざん] | | | 1.69E-02 | 0.87 | | | 低 | 不要 |
| 1.85E-02 | センサー・スマホ間の通信にDDoS攻撃 [(8)Dos:サービス拒否] | | | 1.85E-02 | 1.00 | ネットワーク | 低 | 不要 | 不要 |
| 9.80E-03 | 環境により正しくない血糖値が測定されてしまった [(1) EN:環境要因] | 3.65E-03 | ほとんど発生しない MTBF 1万時間以上をイメージ | 6.17E-03 | 0.00 | | | | |
| 4.24E-02 | センサーの故障により正しくない血糖値が測定されてしまった [(2)FA:機器故障] | 3.65E-02 | 起こり得るが稀 MTBF 1,000時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 9.80E-03 | 測定器のバグによりセンサーの物理値から正しく血糖値に変換されなかった [(3)BG:プログラムのバグ] | 3.65E-03 | ほとんど発生しない MTBF 1万時間以上をイメージ | 6.17E-03 | 0.00 | | | | |
| 3.69E-01 | 測定器の設置方法や使いかたを間違えた [(4)HE:ヒューマンエラー] | 3.65E-01 | 頻繁に起こることが前提 MTBF 100時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 1.85E-02 | IOT機器に成りすました別のIOT機器から間違った情報が | | | 1.85E-02 | 1.00 | ネットワーク | 低 | 不要 | 不要 |

ネットワーク
隣接
ローカル
物理

MTBFなどを選択

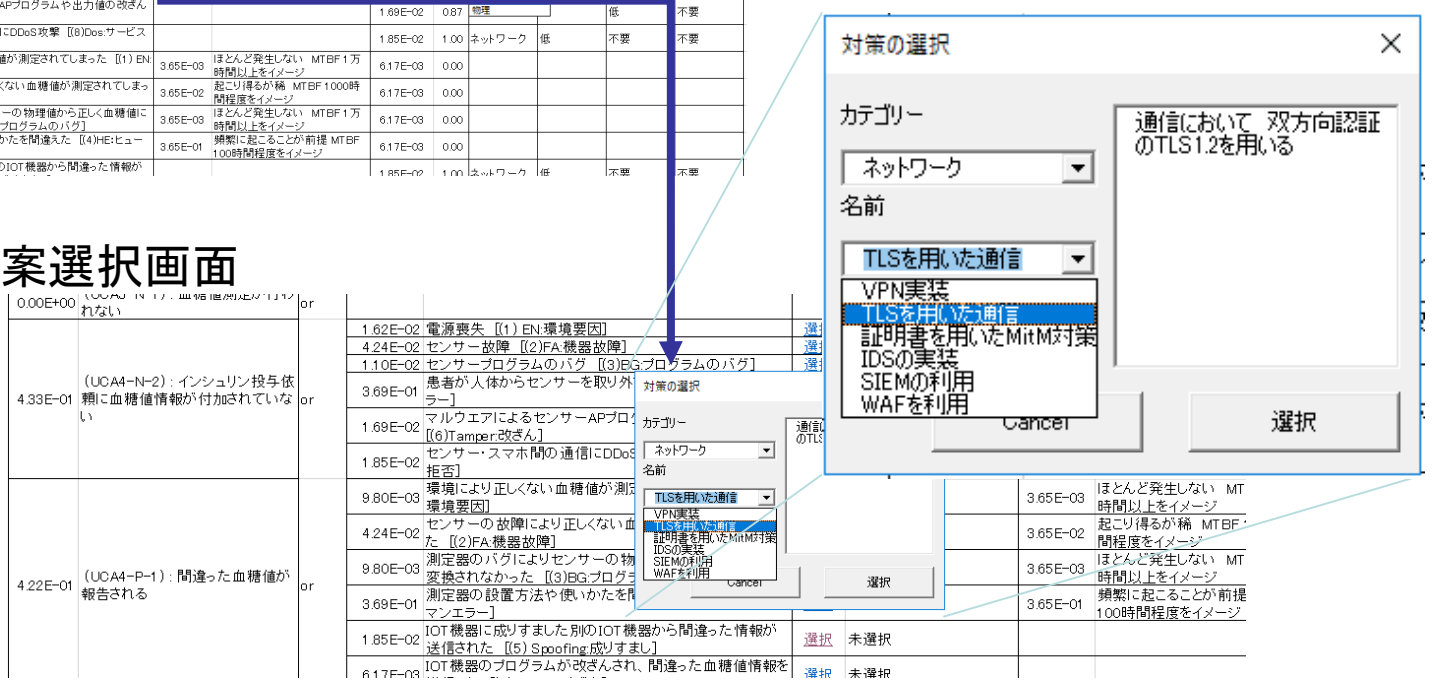
CVSS v3基本評価基準を選択

# 対策案の策定

## 分析画面

| 脅威の原因 | | セーフレベル | | セキュリティレベル | | 攻撃元区分(AV) | 攻撃条件の複雑さ(AC) | 必要な特権レベル(PR) | ユーザー関与レベル(UI) |
|---|---|---|---|---|---|---|---|---|---|
| 1.62E-02 | 電源喪失 [(1) EN:環境要因] | | | 1.62E-02 | 0.82 | ネットワーク | 高 | 不要 | 不要 |
| 4.24E-02 | センサー故障 [(2)FA:機器故障] | 3.65E-02 | 起こり得るが稀 MTBF 1000時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 1.10E-02 | センサープログラムのバグ [(3)BG:プログラムのバグ] | | | 1.10E-02 | 0.39 | ローカル | | 低 | 要 |
| 3.69E-01 | 患者が人体からセンサーを取り外す [(4)HE:ヒューマンエラー] | 3.65E-01 | 頻繁に起こることが前提 MTBF 100時間程度をイメージ | 6.17E-03 | 0.00 | ネットワーク<br>隣接<br>ローカル<br>物理 | | | |
| 1.69E-02 | マルウエアによるセンサーAPプログラムや出力値の改ざん [(6)Tamper:改ざん] | | | 1.69E-02 | 0.87 | | | 低 | 不要 |
| 1.85E-02 | センサー・スマホ間の通信にDDoS攻撃 [(8)Dos:サービス拒否] | | | 1.85E-02 | 1.00 | ネットワーク | 低 | 不要 | 不要 |
| 9.80E-03 | 環境により正しくない血糖値が測定されてしまった [(1) EN:環境要因] | 3.65E-03 | ほとんど発生しない MTBF 1万時間以上をイメージ | 6.17E-03 | 0.00 | | | | |
| 4.24E-02 | センサーの故障により正しくない血糖値が測定されてしまった [(2)FA:機器故障] | 3.65E-02 | 起こり得るが稀 MTBF 1000時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 9.80E-03 | 測定器のバグによりセンサーの物理値から正しく血糖値に変換されなかった [(3)BG:プログラムのバグ] | 3.65E-03 | ほとんど発生しない MTBF 1万時間以上をイメージ | 6.17E-03 | 0.00 | | | | |
| 3.69E-01 | 測定器の設置方法や使いかたを間違えた [(4)HE:ヒューマンエラー] | 3.65E-01 | 頻繁に起こることが前提 MTBF 100時間程度をイメージ | 6.17E-03 | 0.00 | | | | |
| 1.85E-02 | IOT機器に成りすました別のIOT機器から間違った情報が | | | 1.85E-02 | 1.00 | ネットワーク | 低 | 不要 | 不要 |

## 対策案選択画面




各HCF/Threat Case Factorについて、有効な対策案を選択
対策結果資産が自動的に行われる
対策案はDB管理され、再利用可能

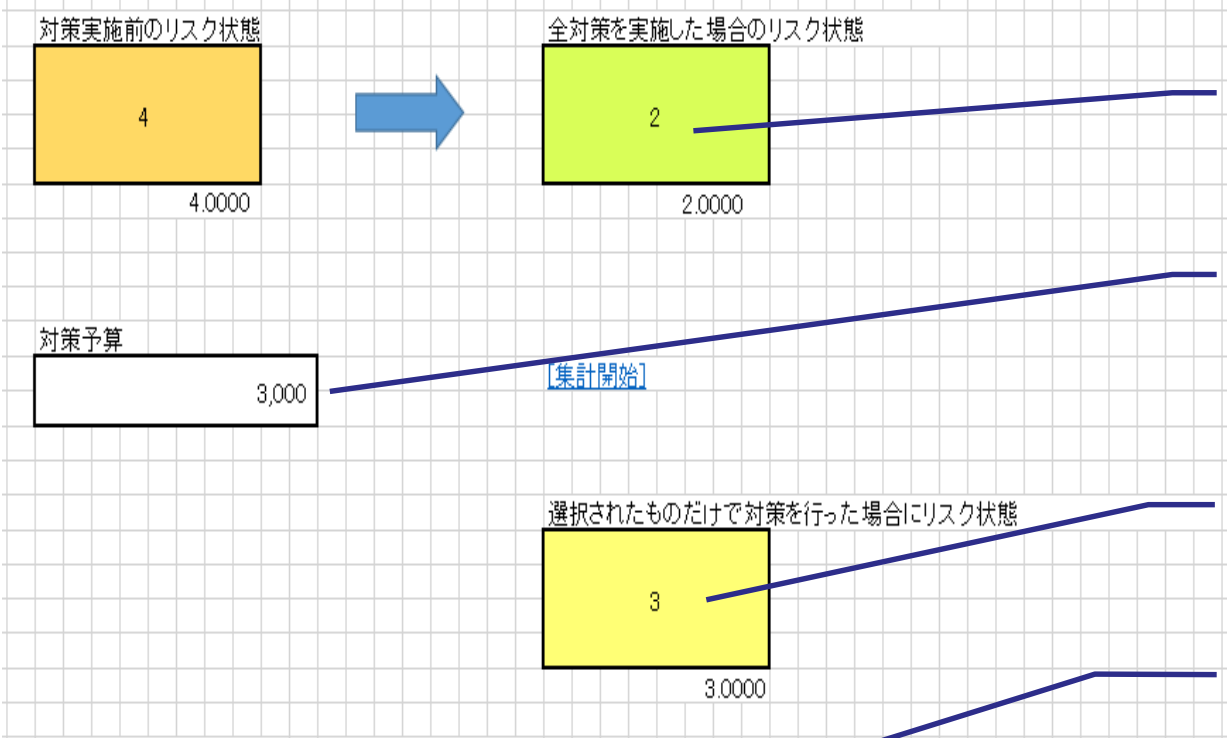
# 対策効果の検討

## 各安全制約（ハザード・脅威）についてリスクを計算

| 安全制約/脅威・ハザード | 原因事象 | ① インシデントの影響 | ② 対策前 発生頻度 | ② 対策前 リスク | ③ 対策後 発生頻度 | ③ 対策後 リスク |
|---|---|---|---|---|---|---|
| (SC1): 血糖値が異常に低下しないようにする<br>・(H1) 血糖値が異常に低下する | (UCA2-T-1) : 血糖値測定指示がセンサーに到達するのに時間がかかりすぎて、測定が正しく行われない | 4 | 5 | 4 | 2 | 2 |
| | (UCA3-N-1) : 血糖値測定が行われない | | | | | |
| | (UCA4-N-2) : インシュリン投与依頼に血糖値情報が付加されていない | | | | | |
| | (UCA4-P-1) : 間違った血糖値が報告される | | | | | |
| | (UCA5-P-1) : 間違った血糖値が報告される | | | | | |
| | (UCA5-P-3) : 血糖値情報が正しくないスマホから送信される | | | | | |
| | (UCA5-T-1) : 受信相手の認証処理が済む前に血糖値情報を送信してしまう | | | | | |
| | (UCA6-P-1) : 間違った血糖値が医師に報告される | | | | | |
| | (UCA6-P-2) : 血糖値情報が正しくない医師や医師でない第三者に送信される | | | | | |
| | (UCA6-P-3) : 血糖値情報が、正しくないPCから医師に提供される | | | | | |
| | (UCA6-T-1) : 血糖値情報が届く前にインシュリン投与依頼が医師に送信される | | | | | |
| | (UCA7-P-1) : 投与する必要のない患者に投与指示をだしてしまう | | | | | |
| | (UCA8-P-1) : 間違った投与指示がスマホに届く | | | | | |
| | (UCA10-P-1) : 間違えたIOT機器にインシュリン投与指示が届く | | | | | |
| | (UCA10-P-2) : 間違ったスマホからIOT機器にインシュリン投与指示が届く | | | | | |

① アクシデント・インシデントが起きた時のインパクトで設定したレベル値の平均を表示
② 対策前の発生頻度とリスクレベル値を計算して表示
③ 対策実施後に期待される発生頻度とリスクレベル値を計算して表示

# 費用対効果の算出と実施優先順位




単体ROI順の対策案一覧　[選択を反映して再計算]

（グレーアウトは、対策予算で対応できないもの　左の*で手動選択）

| | ID | 対策名 | 説明 | 費用 | 効果 | ROI値 |
|---|---|---|---|---|---|---|
| * | 15 | AES256を利用 | AES暗号に256の鍵長を用いる | 600 | 0.747201077 | 1.25E-03 |
| * | 14 | APIコールに認証を設定 | APIコールを行う前にコーラーの確認を行う | 1000 | 0.759754743 | 7.60E-04 |
| * | 6 | 多要素認証(パスワードと | ユーザーが関与する処理において、パス | 300 | 8.18E-02 | 2.73E-04 |
| * | 2 | バッファーオーバーフロー | Stack Smash Protectionの利用 | 200 | 2.41E-02 | 1.21E-04 |
| * | 11 | MACによる認証 | ノードからのアクセスに対してMACを使った | 500 | 4.35E-02 | 8.69E-05 |
| * | 5 | 証明書を用いたMitM対策 | 通信を確立するまえに証明書を用いて相手 | 200 | 1.37E-02 | 6.87E-05 |
| | 22 | ペネトレーションテスト（ | ハードウエアの破壊を伴うペネトレーション | 3000 | 6.99E-02 | 2.33E-05 |
| | 1 | VPN実装 | ノード間での通信にVPNを利用 | 1000 | 1.22E-02 | 1.22E-05 |

選択したすべての対策を実施した場合おリスク状態

予算に上限がある場合に入力

予算内で実施した場合のリスク状態

実施する対策の一覧
- 費用対効果の高い準にソート
- グレーアウトは、予算的理由で実施できないもの
- 各費用対効果は、その対策のみを行ったときの全体リスクへの影響で評価
- 先頭の＊を変更することで、選択項目を変更して再計算可能

# 適用による感想

1. STAMP/STPAの活用領域の拡大に寄与
   STAMP/STPAにより抽出されるHCFやThreat Cause Factorを
   対策案策定・優先順位の決定・実施に活用できた
   → IoT機器へのアセスメントなどで実業務への適用が可能

2. SecurityとSafetyを同時に扱い、脅威して分析できるSTAMP/STPAと
   Fault / Attack Tree分析を融合することで、より網羅性の高い、
   準定量分析が可能となった

3. 実業務で用いる具体例について分析すると、小規模なものでも、
   安全制約は数十におよび、それに紐づくHCFやThreat Case Factor、
   合計数百程度以上になる。 MRC4IoTでは、共通入力項目のリンクや
   DB化により入力の軽減を行っているが、さらなる自動化や入力補助手
   法の検討が必要

# まとめ

- ✓ IoT機器のためのリスクコミュニケーションを円滑に行うためのツール
  MRC4IoTを開発

- ✓ MRC4IoTは、リスク分析手法として
  - STAMP STPA
  - Fault Tree/ Attack Tree 分析
  - リスク指向分析

  を利用

- ✓ STAMP STPA部分の分析に STAMP Workbench を活用

- ✓ 医療機器（インシュリンポンプ）や自動車の E/Eシステム(Virtual Car Keyシステム）を用いて分析

ご清聴ありがとうございました