

# サイバーセキュリティと リスクマネジメント

東京電機大学未来科学部教授  
会計検査院最高情報セキュリティアドバイザー  
佐々木良一

sasaki@im.dendai.ac.jp



# 本日の内容

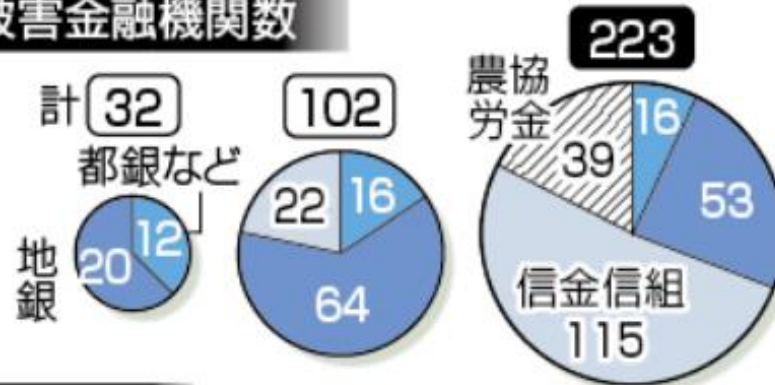
---

1. サイバーセキュリティの最近の動向
2. リスク評価の動向
3. 多重リスクコミュニケーターの開発
4. IoTを含むシステムへのリスク評価法の考察
5. 今後の方向



# インターネットバンキングの被害

被害金融機関数



被害額

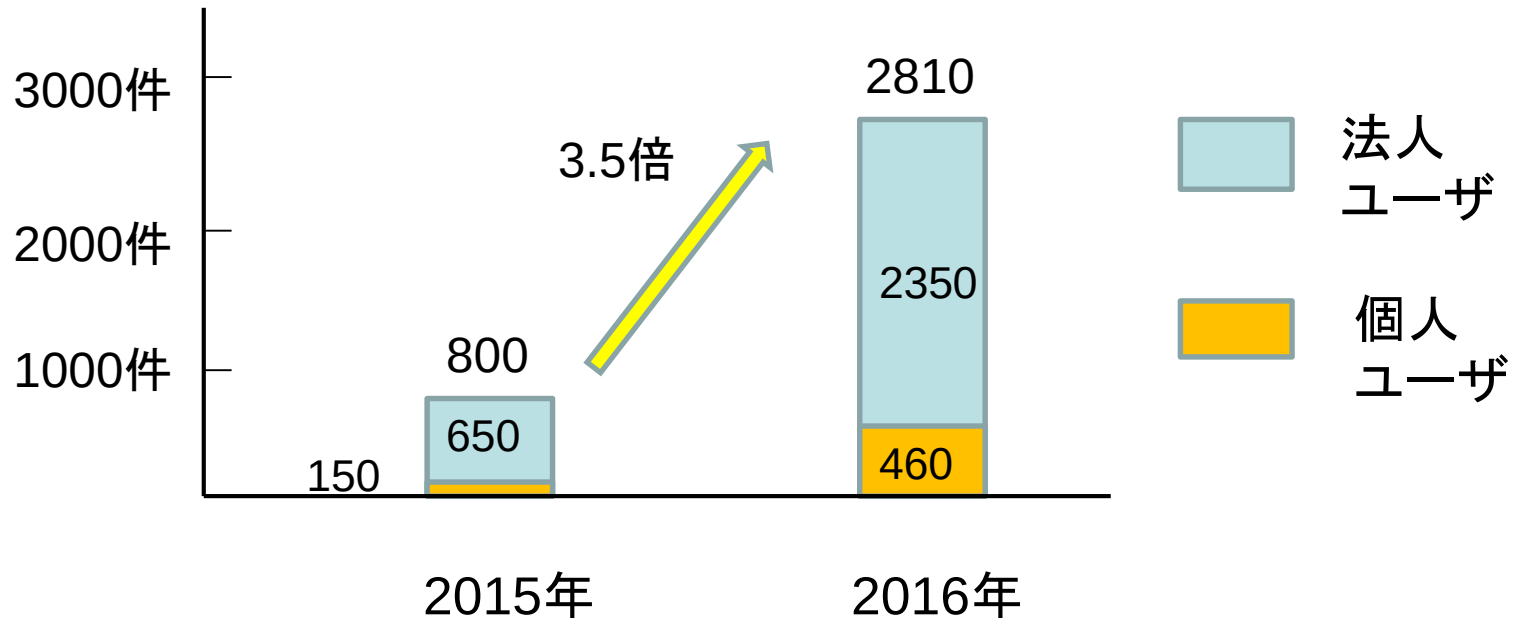


[http://www.jiji.com/jc/graphics?p=ve\\_soc\\_network-bankfuseisoukin](http://www.jiji.com/jc/graphics?p=ve_soc_network-bankfuseisoukin)

# ランサムウェアの被害動向

ランサムウェア  
被害報告件数

トレンドマイクロ調査結果



<https://scan.netsecurity.ne.jp/article/img/2017/03/03/39509/21918.html>

# サイバー攻撃の歴史

---

## ＜セキュリティにとっての第一のターニングポイント＞

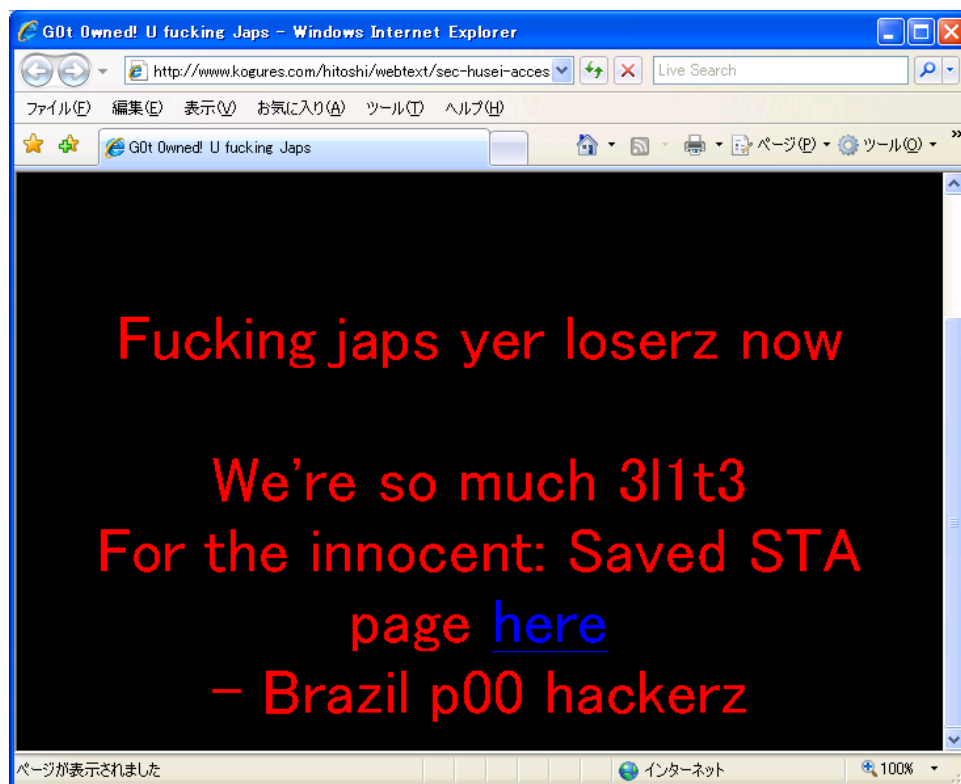
- 2000年 科学技術庁などのホームページの改ざん事件
- 2000年 不正アクセス禁止法施行
- 2000年 JNSA発足(2001年NPO化)
- 2001年 Code Red、Sircumによる被害
- 2001年 電子署名法施行
- 2001年 CRYPTREC(暗号技術検討会)発足

## ＜セキュリティにとっての第二のターニングポイント＞

- 2010年 Stuxnetの出現(遠心分離機への攻撃)
- 2011年 ウイルス作成罪施行
- 2011年 三菱重工などへの標的型メール攻撃
- 2015年 日本年金機構への攻撃



# 科学技術庁ホームページ改ざん事件



2000年1月

Reference : <http://www.kogures.com/hitoshi/webtext/sec-husei-access/homepage.html>

# サイバー攻撃の歴史

---

## ＜セキュリティにとっての第一のターニングポイント＞

- 2000年 科学技術庁などのホームページの改ざん事件
- 2000年 不正アクセス禁止法施行
- 2000年 JNSA発足(2001年NPO化)
- 2001年 Code Red、Sircumによる被害
- 2001年 電子署名法施行
- 2001年 CRYPTREC(暗号技術検討会)発足

## ＜セキュリティにとっての第二のターニングポイント＞

- 2010年 Stuxnetの出現(遠心分離機への攻撃)
- 2011年 ウイルス作成罪施行
- 2011年 三菱重工などへの標的型メール攻撃
- 2015年 日本年金機構への攻撃



# 2つのターニングポイントの比較

|        | 第一次ターニングポイント(2000年ごろ) | 第二次ターニングポイント(2010年以降)                |
|--------|-----------------------|--------------------------------------|
| 攻撃目的   | 面白半分                  | 多様化(面白半分、主義主張、お金儲け、国家の指示)            |
| 攻撃者    | ハッカー(クラッカー)           | ハッカー、ハクティビスト、犯罪者、スパイ、軍人              |
| 攻撃対象   | WEBなどの一般IT            | 重要情報インフラも<Stuxnet>                   |
| 攻撃パターン | 不特定多数                 | <u>標的型</u> <Stuxnet、ソニー、三菱重工、日本年金機構> |
| 攻撃技術   | 低一中                   | 中一高 <Stuxnet、ソニー、三菱重工、農林水産省 >        |

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ

# 目次

---

1. サイバーセキュリティの最近の動向
2. ITシステムのリスク評価の動向
3. 多重リスクコミュニケーターの開発
4. IoTを含むシステムへのリスク評価法の  
考察
5. 今後の方向



# セキュリティ評価のアプローチ法

---

## ＜従来＞

- (i) 脅威を重視したアプローチ
- (ii) 資産を重視したアプローチ
- (iii) 脆弱性を重視したアプローチ

## ＜今後＞

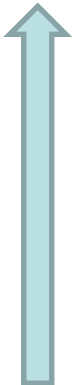
### リスクを重視したアプローチ

$$\text{リスク} = \text{資産} \times \text{脆弱性} \times \text{脅威}$$

# 評価のアプローチ法

| アプローチ法 | 長所                 | 欠点                       |
|--------|--------------------|--------------------------|
| 定量的    | 費用対効果分析を最も効果的に支援   | 得られた数値または結果に関する信頼性の説明が必要 |
| 半定量的   | 比較的少ないコストで相互比較が可能に | 厳密性が不足                   |
| 定性的    | 分析にコストがかからない       | 経験により結果が異なる場合もある         |

今後の方向

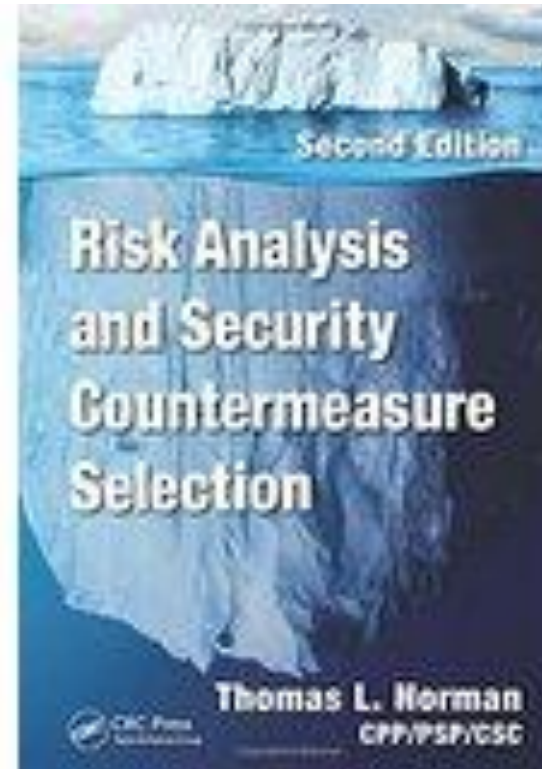


FIPS SP 800-30を参考に作成

# 文献

---

- Thomas L. Norman “Risk Analysis and Security Countermeasure” CRC Press, 2016



定量的リスク評価を扱う本は増えてきている。

# ITシステムの安全の階層化

| 階層 | 対象               | 扱う事故・障害               | 従来の学問・技術分野               | 指標                  |
|----|------------------|-----------------------|--------------------------|---------------------|
| 3  | ITシステムが行うサービスの安全 | 発券サービスの停止、プライバシーの喪失など | システム工学<br>リスク学<br>社会科学など | プライバシー、ユーザビリティ      |
| 2  | ITシステムが扱う情報の安全   | 情報のCIAの喪失             | セキュリティ                   | セキュリティ(機密性、完全性、可用性) |
| 1  | ITシステムそのものの安全    | コンピュータや通信機器の故障        | 信頼性工学<br>セキュリティ          | リライアビリティ、アベイラビリティ   |

\* 従来情報セキュリティが扱っていた範囲

# ITシステムの安全の階層化

| 階層 | 対象               | 扱う事故・障害             | 従来の学問・技術分野               | 指標                  |
|----|------------------|---------------------|--------------------------|---------------------|
| 3  | ITシステムが行うサービスの安全 | 発生サービスの停止<br>プライバシー | システム工学<br>リスク学<br>社会科学など | プライバシー、ユーザビリティ      |
| 2  | ITシステムが扱う情報の安全   | 情報のCIAの喪失           | セキュリティ                   | セキュリティ(機密性、完全性、可用性) |
| 1  | ITシステムそのものの安全    | コンピュータや通信機器の故障      | 信頼性工学<br>セキュリティ          | リライアビリティ、アベイラビリティ   |

トラスト

ITリスク

ニューディペンダビリティ

\* 従来情報セキュリティが扱っていた範囲

# リスクとは



1. リスクとは、英語のRiskの訳であり、危険と訳される場合もある。「将来の帰結に対する現在における予測」という見方が下敷きになっていて常に不確実性を伴う。

2. 工学分野の確率論的リスク評価では通常次のように定義することが多い。

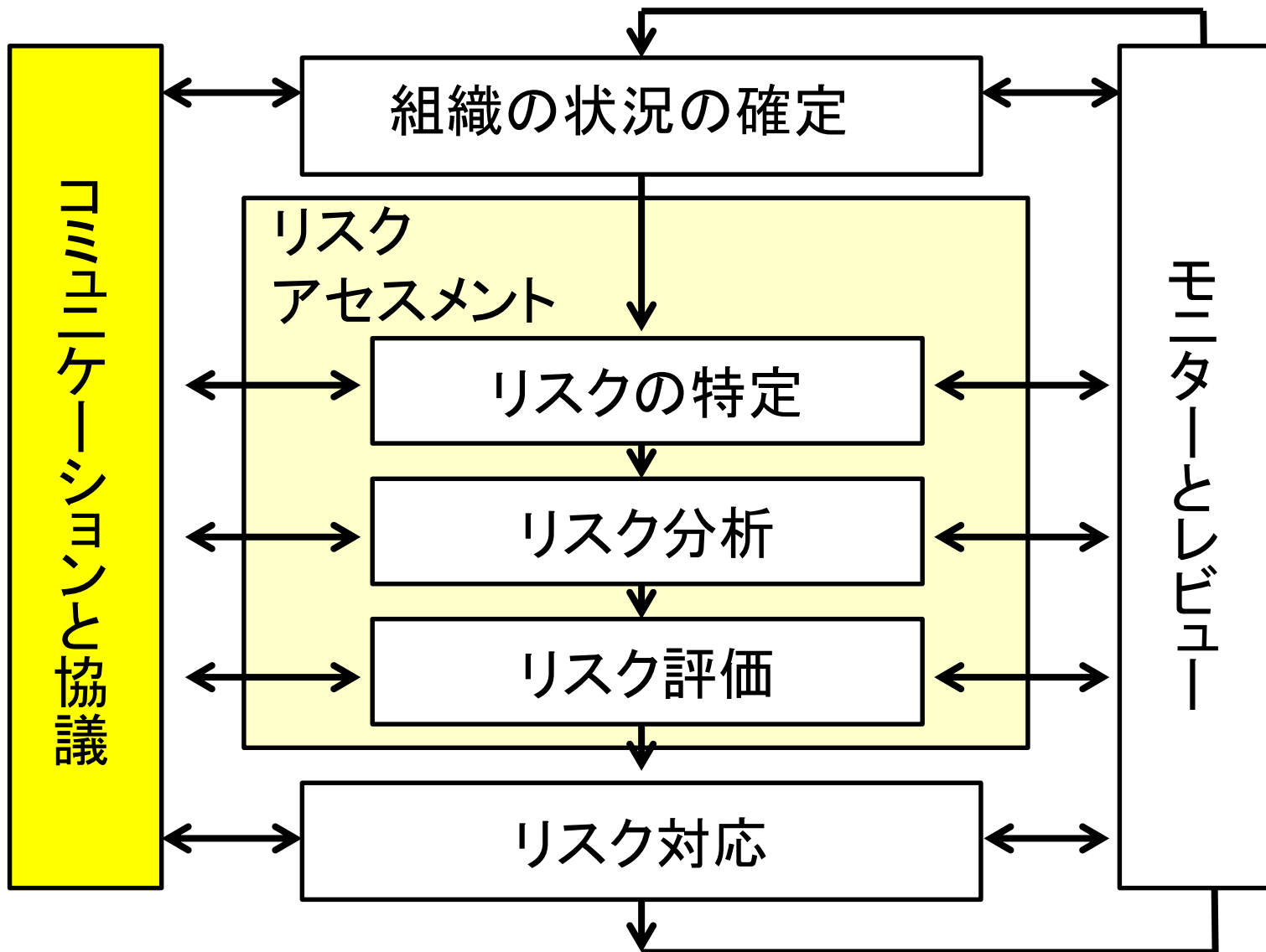
リスク＝損害の大きさ × 損害の発生確率

3. 「ISO/IEC 27005:2008」ではITのリスクを以下のように定義しているが、結局同じことを表している。

リスク＝資産価値 × 脅威 × 脆弱性

(注) 英語のRiskが登場するのは1660年代。ハザードや災いを意味するイタリア語risicoからの転用

# リスクマネジメントのプロセスの流れ



# 目次

---

1. サイバーセキュリティの最近の動向
2. ITシステムのリスク評価の動向
3. 多重リスクコミュニケーターの開発
4. IoTを含むシステムへのリスク評価法の  
考察
5. 今後の方向



# 代表的ITリスクの現状の調査

1. 2000年問題
2. 個人情報漏洩リスク
3. 暗号の危殆化リスク
4. サイバーテロのリスク
5. 大規模情報システム故障のリスク

詳細は、佐々木良一「ITリスクの考え方」岩波新書、2008第2章、第4章参照



# 多重リスクコミュニケーター(MRC)の対応

## <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. 多くの関係者(経営者・顧客・従業員など)が存在⇒多くの関係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制約条件とし、残存リスク等を最小化する対策組み合わせ問題として定式化

②関係者の合意が得られるまで制約条件値などの値を変えつつ最適化エンジンを用い求解



専門家

対策案

①②③④

定式化  
結果

多重リス  
クコミュニ  
ケーター  
MRC

最適解  
対策案  
①③の  
組合せ

END

満足

制約条件などの変更

ファシリテーター

関係者



# MRCの適用

## ①適用対象(組織内合意)

(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人までの組織内合意形成問題なら基本的有効性を確認

## ②受賞

日本セキュリティ・マネジメント学会2009年度論文賞受賞  
など

## ③招待講演

IEEE主催のCFSE2012 Keynote Speech など

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

# MRCに関する最近の研究



## 1. 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ー
- (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ー
- (5) IoTを含むシステムへの機能拡張

## 2. 合意形成対象者が1000人を超える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)

# 目次

---

1. サイバーセキュリティの最近の動向
2. リスク評価の動向
3. 多重リスクコミュニケーターの開発
4. IoTを含むシステムへのリスク評価法の  
考察
5. 今後の方向



# IoTとは

- IoT とは”Internet of Things”の略。
- ITU(国際電気通信連合)の勧告(ITU-T Y.2060(Y.4000))では、「情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラ」
- 1999年にケビン・アシュトン(Kevin Ashton)が命名。

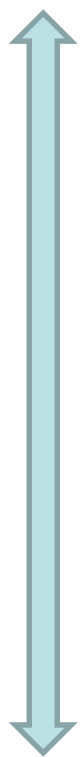


ここで「もの」とは、IPアドレスを持つ防犯カメラや各種センサーなど多様(PCはものだが通常対象外)

# 接続される主要な「もの」

---

システムレベル



- (1) 重要インフラの制御システム
- (2) スマートハウス
- (3) 自動車
- (4) 情報家電
- (5) 複合機
- (6) 電子掲示板
- (7) 防犯カメラ
- (8) スマートセンサー

部品レベル



# IoTのセキュリティが重要になった背景

---

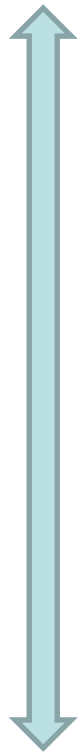
1. IoTが急速に普及していくことが予想される。  
2020年には500億個（インテルの予測）
2. IoTの機能喪失の影響が大きい（人命が失われる場合も）
3. IoTシステムが被害にあうだけではなく、IoT装置が踏み台になった攻撃の可能性も大
4. 現状のシステムでは一般に対策が困難（性能の制約や自動アップグレードの困難性等）



# 接続される主要な「もの」

---

システムレベル



(1) 重要インフラの制御システム

(2) スマートハウス

(3) 自動車

(4) 情報家電

(5) 複合機

(6) 電子掲示板

(7) 防犯カメラ

(8) スマートセンサー

部品レベル



# 電力会社へのサイバー攻撃で140万世帯が停電

2015年12月23日に、ウクライナ西部の都市イヴァーノ=フランクィウシク周辺で140万世帯が停電しました。停電自体は数時間のことでしたが、これが実はサイバー攻撃によるもので、「BlackEnergy」と呼ばれるマルウェアを用いたモノであることが明らかになっています。

これはウクライナのエネルギー省が明かしたものの。以前から、インフラを狙ったサイバー攻撃については警鐘が鳴らされていましたが、本件はサイバー攻撃が実際に成功した極めて珍しい事例です。

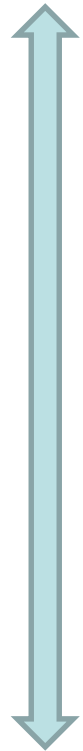
<http://gigazine.net/news/20160106-blackenergy-trojan/>



# 接続される主要な「もの」

---

システムレベル



- (1) 重要インフラの制御システム
- (2) スマートハウス
- (3) 自動車
- (4) 情報家電
- (5) 複合機
- (6) 電子掲示板
- (7) 防犯カメラ
- (8) スマートセンサー

部品レベル



# 自動車への具体的攻撃例

- Blackhat2015でCharlie Miller氏とChris Valasek氏がジープのチェロスキーの遠隔操作法を発表



攻撃者は数マイル  
離れた自宅から

ハンドル操作  
ブレーキの無効化  
高速走行中のエン  
ジンの停止など

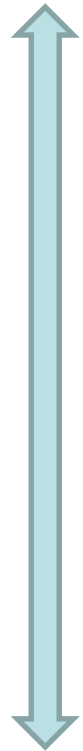
140万台のリ  
コールに

<https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/>

# 接続される主要な「もの」

---

システムレベル



- (1) 重要インフラの制御システム
- (2) スマートハウス
- (3) 自動車
- (4) 情報家電
- (5) 複合機
- (6) 電子掲示板
- (7) 防犯カメラ
- (8) スマートセンサー

部品レベル



# 無防備な防犯カメラの監視映像

## < Insecam サイト >



Watch PanasonicHD camera in  
Japan  
Tokyo



Watch PanasonicHD camera in  
Japan  
Tokyo



Watch PanasonicHD camera in  
Japan  
Tokyo



Watch Panasonic camera in  
Japan  
Tokyo



Watch Panasonic camera in  
Japan  
Tokyo



Watch Panasonic camera in  
Japan  
Sendai

<http://animeblog.hatenablog.jp/entry/2016/01/20/084826>

# その他のIoTのセキュリティ

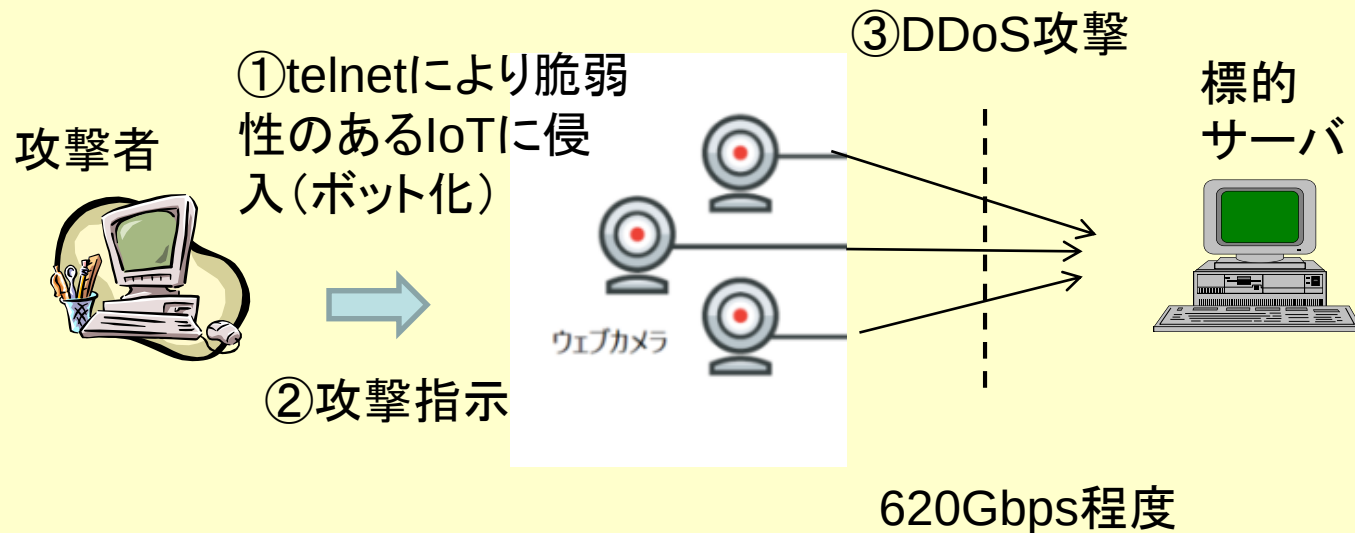
---

- 防犯カメラ、家庭用ルータなどがアクセス管理が不十分なため攻撃の踏み台に
- 今後は家庭用ロボットなどのハッキングによる被害なども発生か



# IoTを利用したDDoS攻撃

## ＜MiraiによるDDoS攻撃＞



DDoS (Dissributed Denial Of Service) 攻撃 (サービス不能攻撃ともいう)

# IoTセキュリティガイドラインの制定

## 5つの指針・21の要点(1)

| 大項目 | 指針                         | 要点                                  |
|-----|----------------------------|-------------------------------------|
| 方針  | 指針1<br>IoTの性質を考慮した基本方針を定める | 要点1. 経営者がIoTセキュリティにコミットする           |
|     |                            | 要点2. 内部不正やミスに備える                    |
| 分析  | 指針2<br>IoTのリスクを認識する        | 要点3. 守るべきものを特定する                    |
|     |                            | 要点4. つながることによるリスクを想定する              |
|     |                            | 要点5. つながりで波及するリスクを想定する              |
|     |                            | 要点6. 物理的なリスクを認識する                   |
|     |                            | 要点7. 過去の事例に学ぶ                       |
| 設計  | 指針3<br>守るべきものを守る設計を考える     | 要点8. 個々でも全体でも守れる設計をする               |
|     |                            | 要点9. つながる相手に迷惑をかけない設計をする            |
|     |                            | 要点10. 安全安心を実現する設計の整合性をとる            |
|     |                            | 要点11. 不特定の相手とつなげられても安全安心を確保できる設計をする |
|     |                            | 要点12. 安全安心を実現する設計の検証・評価を行う          |

IoTセキュリティガイドライン 平成28年7月 座長 佐々木良一

[http://www.soumu.go.jp/main\\_content/000428393.pdf](http://www.soumu.go.jp/main_content/000428393.pdf)

# IoTセキュリティガイドラインの制定

## 5つの指針・21の要点(2)

|       |                               |                                                 |
|-------|-------------------------------|-------------------------------------------------|
| 構築・接続 | 指針4<br>ネットワーク上での<br>対策を考える    | 要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける              |
|       |                               | 要点 14. 機能及び用途に応じて適切にネットワーク接続する                  |
|       |                               | 要点 15. 初期設定に留意する                                |
|       |                               | 要点 16. 認証機能を導入する                                |
| 運用・保守 | 指針5<br>安全安心な状態を維持し、情報発信・共有を行う | 要点 17. 出荷・リリース後も安全安心な状態を維持する                    |
|       |                               | 要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える |
|       |                               | 要点 19. つながることによるリスクを一般利用者に知ってもらう                |
|       |                               | 要点 20. IoT システム・サービスにおける関係者の役割を認識する             |
|       |                               | 要点 21. 脆弱な機器を把握し、適切に注意喚起を行う                     |

IoTセキュリティガイドライン 平成28年7月 座長 佐々木良一  
[http://www.soumu.go.jp/main\\_content/000428393.pdf](http://www.soumu.go.jp/main_content/000428393.pdf)

# IoTセキュリティガイドラインの制定

## 5つの指針・21の要点(2)

|       |                                     |                                                                          |
|-------|-------------------------------------|--------------------------------------------------------------------------|
| 構築・接続 | 指針4<br>ネットワーク上で<br>対策を考える           | <p>これらは、一般的IoTのセキュリティに関するガイド</p> <p>個別のIoTシステムの安全対策のためには、個別のリスク評価が必要</p> |
| 運用・保守 | 指針5<br>安全安心な状態<br>維持、情報発信・<br>有を行う  |                                                                          |
|       | 要点 19. つながることによるリスクを一般利用者に知ってもらう    |                                                                          |
|       | 要点 20. IoT システム・サービスにおける関係者の役割を認識する |                                                                          |
|       |                                     | 要点 21. 脆弱な機器を把握し、適切に注意喚起を行う                                              |

IoTセキュリティガイドライン 平成28年7月 座長 佐々木良一  
[http://www.soumu.go.jp/main\\_content/000428393.pdf](http://www.soumu.go.jp/main_content/000428393.pdf)

# IoTを含むシステムのリスク評価の特徴

## 1. ITシステムのリスク評価:

情報のCIAからなるSecurityを中心にする評価

IoTを含む場合は制御対象のリスク評価:

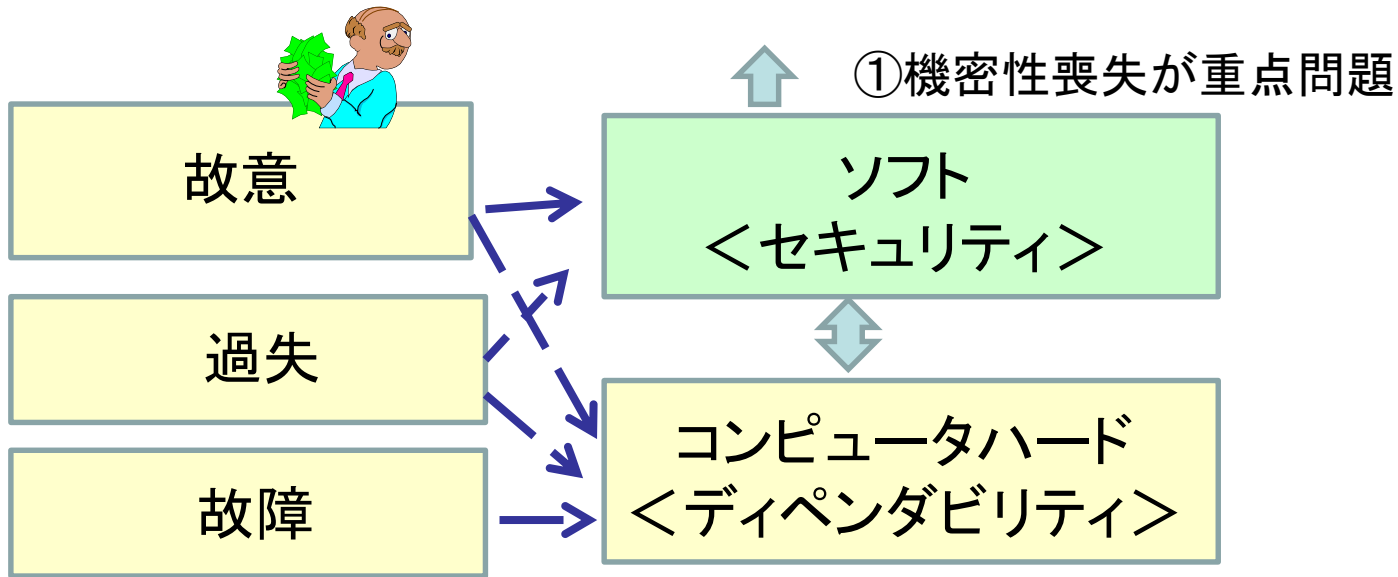
Safetyを主にしSecurityに従にする評価が必要に

2. IoTの種類によっては、センサー系の異常や制御系の異常への対処も重要になる

3. 対策効果の評価まで行う場合は、いろいろなレイヤーでの対策を考慮すべき

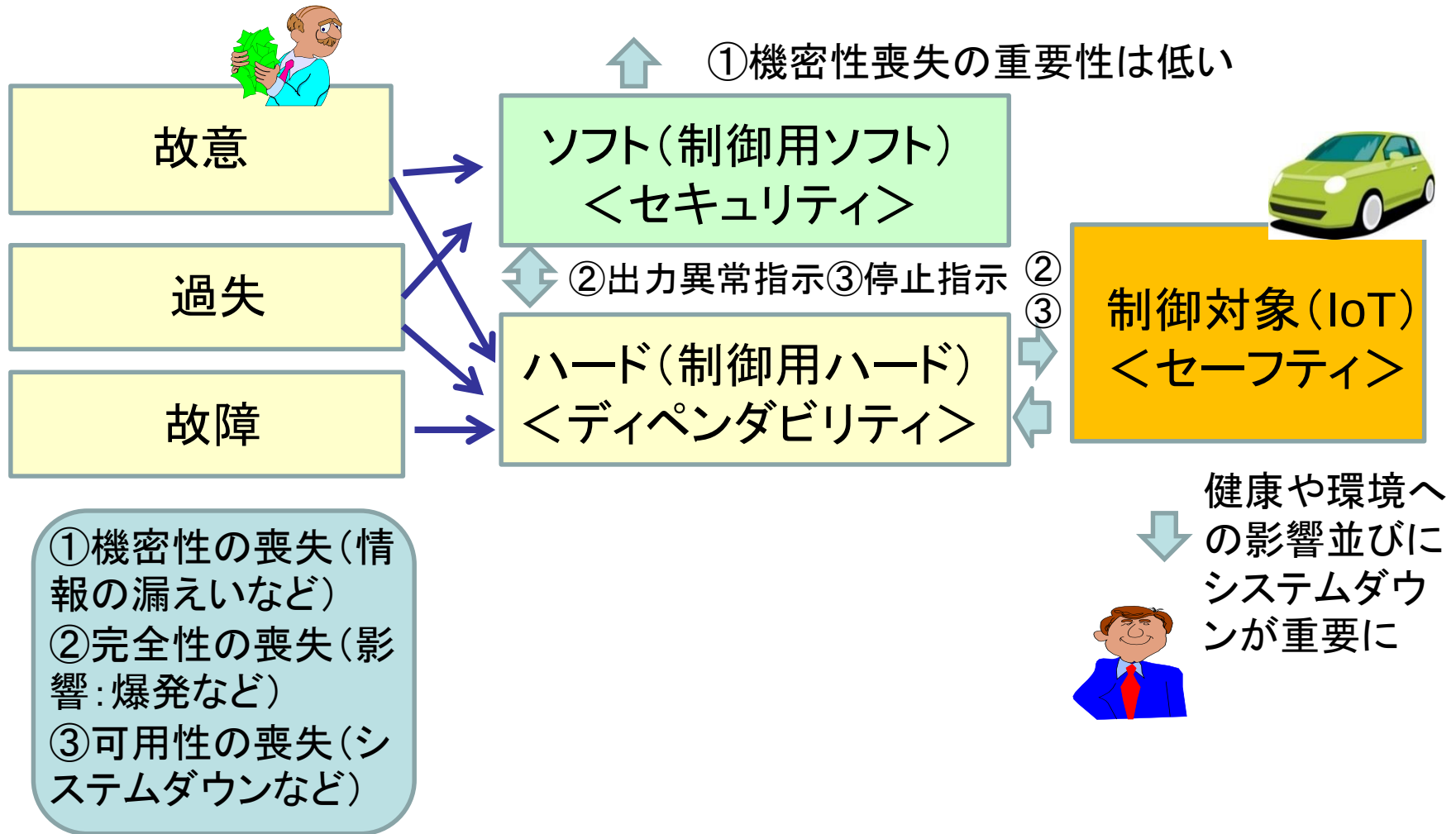


# ITのセキュリティ

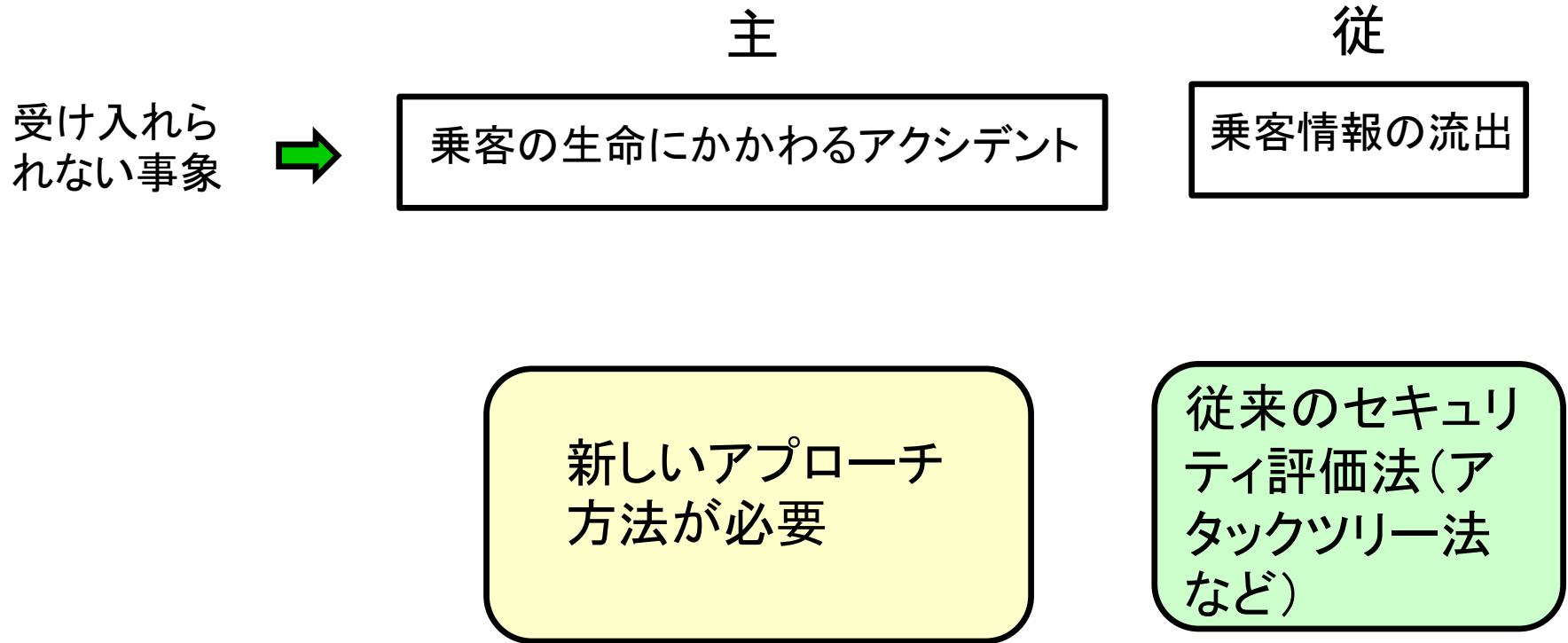


- ①機密性の喪失(情報の漏えいなど)
- ②完全性の喪失(影響:爆発など)
- ③可用性の喪失(システムダウンなど)

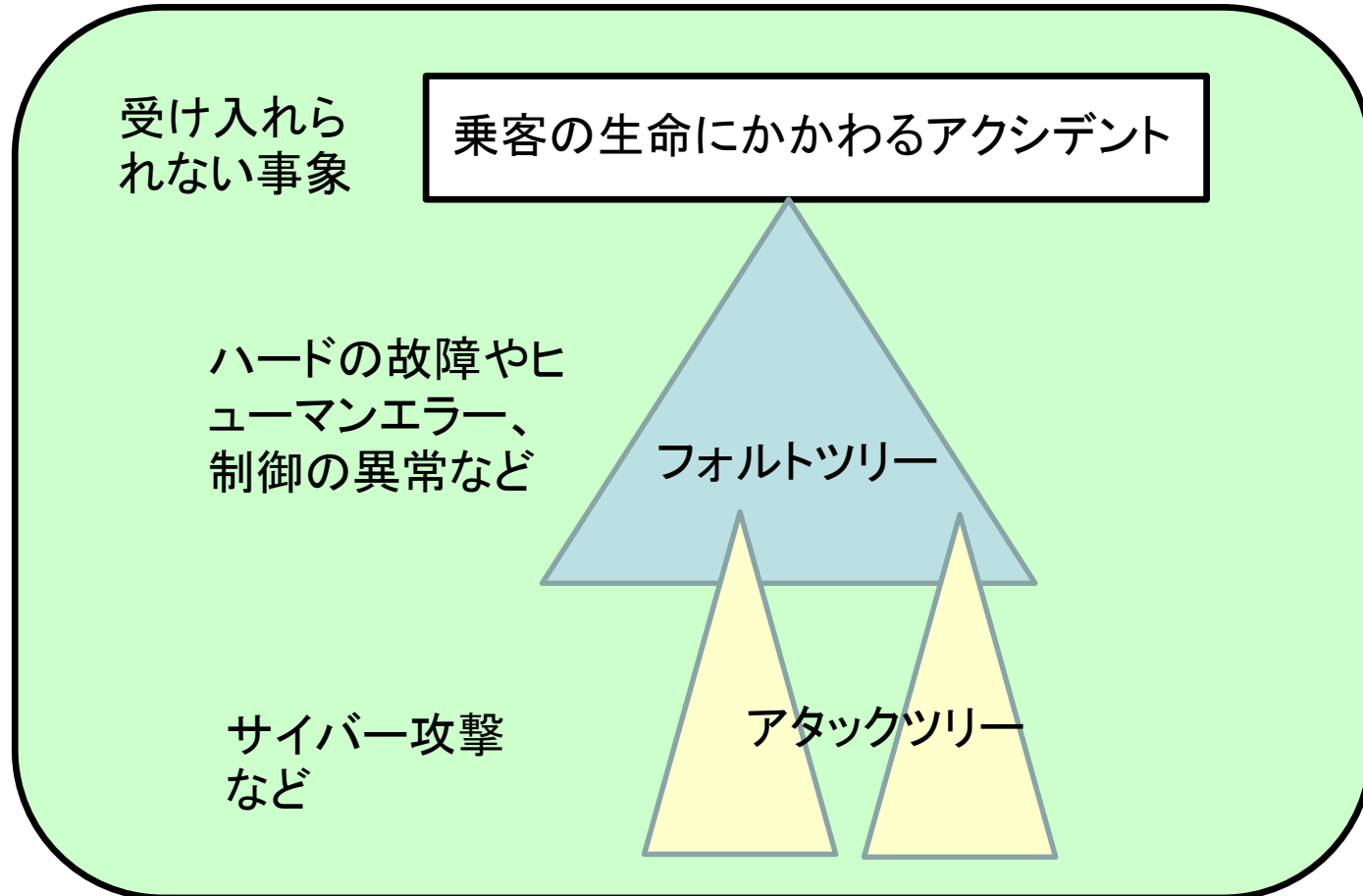
# IoTのセキュリティとセーフティ



# アプローチ方法の概要（航空機データ通信システムの場合）



# アプローチ方法の概要（航空機データ通信システムの場合）



[http://www.jssm.net/wp/wp-content/uploads/2014/04/ITリスク学研究会\\_発表資料\\_2017-08-02-公開用.pdf](http://www.jssm.net/wp/wp-content/uploads/2014/04/ITリスク学研究会_発表資料_2017-08-02-公開用.pdf) (産総研田口氏資料)を参考に作成

# IoTを含むシステムのリスク評価の特徴

## 1. ITシステムのリスク評価:

情報のCIAからなるSecurityを中心

IoTを含む場合は制御対象のリスク評価:

Safetyを主にしSecurityを従にする評価が必要に

## 2. IoTの種類によっては、センサー系の異常や制御系の異常への対処も重要になる

## 3. 対策効果の評価まで行う場合は、いろいろなレイヤーでの対策を考慮すべき



# IoT機器の機能による分類

## 1. ネットワーク側に出力中心のIoT機器(センサー系)

(a) 速度センシング情報など(部品レベル)

(b) 自動車の位置情報など(製品レベル)

(c) タクシーの稼働状況など(システムレベル)

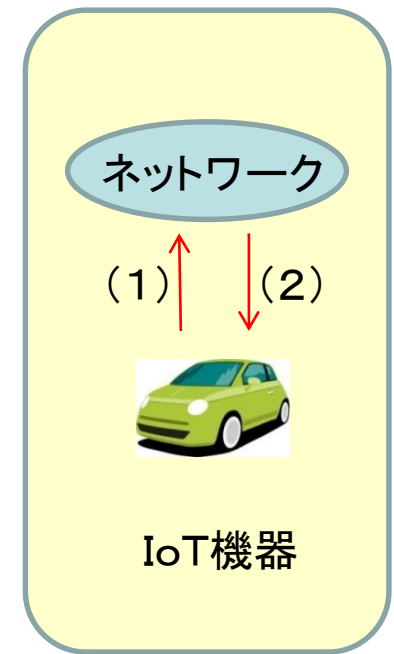
## 2. ネットワーク側から入力中心のIoT機器

(a) 状態表示系

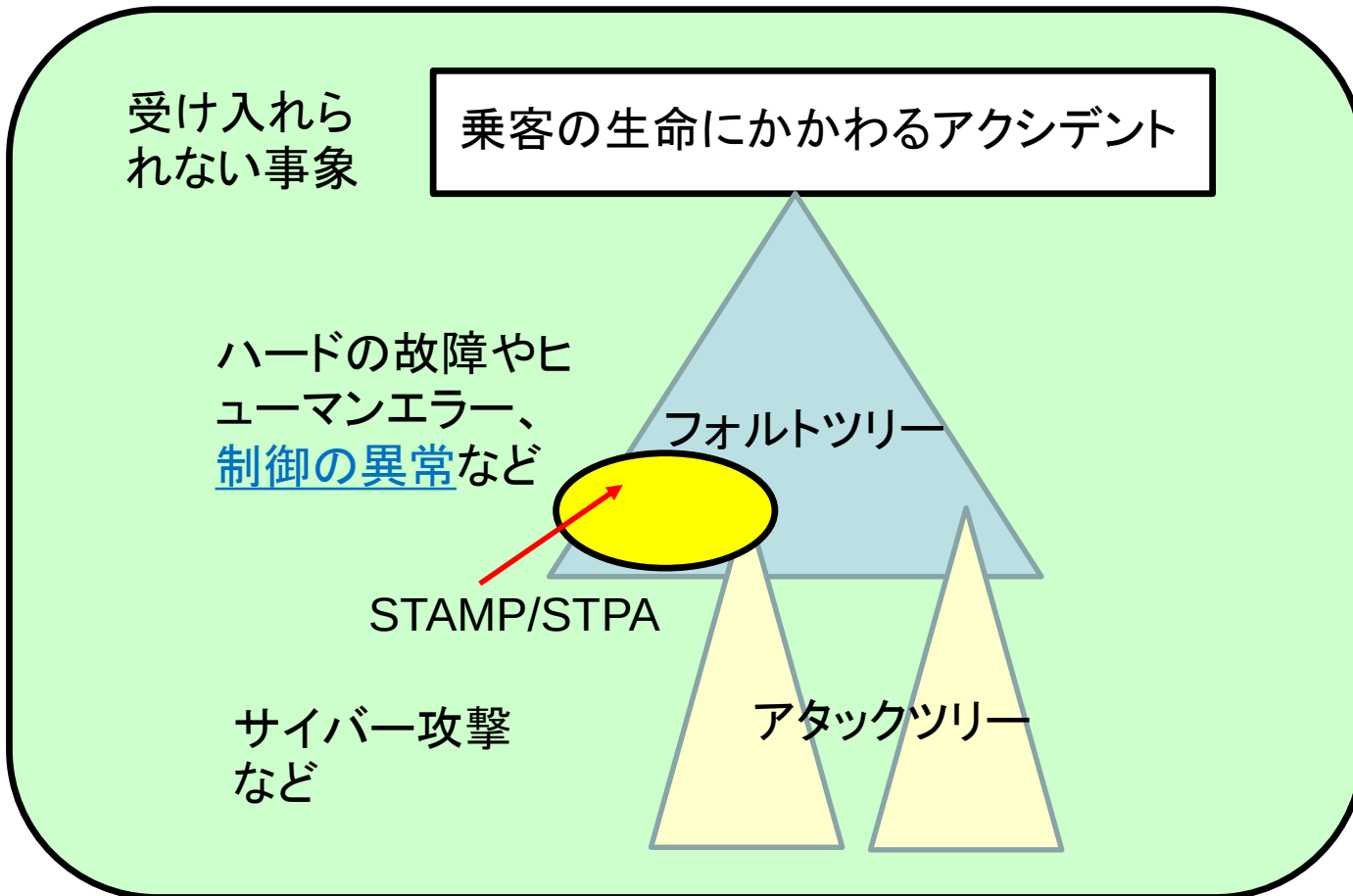
経路ガイドなど

(b) 制御系

速度制限制御など



# アプローチ方法の概要（航空機データ通信システムの場合）



STAMP/STPAについては

<https://www.ipa.go.jp/files/000055009.pdf> などを参照

# STAMP/STPAとは

## ■ STAMP/STPA

### システムアプローチに基づく新たな安全解析手法

- STAMP (**S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocess) : システム理論に基づく事故モデル
- STPA (**ST**AMP based **P**rocess **A**nalysis) : STAMPに基づく安全解析手法

■ マサチューセッツ工科大学(MIT)のNancy G. Leveson教授が、“Engineering a Safer World (2012)”の中で提唱

- 複数のコントローラが介在する複雑なシステム(Complicated system)に対する安全解析の方法論
- システムを構成するサブシステムやコンポーネントに不具合がなくとも、サブシステムやコンポーネントの組み合わせによって全体のシステムにおける不具合が発生する

プロセス

システム工学(例 仕様記述、安全性ガイド設計、設計原理)

リスク管理

管理の原則/組織設計

運用

規制

ツール(手法)

事故/イベント分析(CAST)

ハザード分析(STPA)

早期概念分析(STECA)

組織的/文化的リスク分析

先行指標識別

セキュリティ分析(STPA-Sec)

STAMP: 安全解析方法論



**Engineering a Safer World**  
Systems Thinking Applied to Safety  
By Nancy G. Leveson  
January 2012

# STAMP/STPAとは

## ■ STAMP/STPA

### システムアプローチに基づく新たな安全解析手法

- STAMP (**S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocess) : システム理論に基づく事故モデル
- STPA (**S**TAMP based **P**rocess **A**nalysis) : STAMPに基づく安全解析手法

■ マサチューセッツ工科大学(MIT)のNancy G. Leveson教授が、“Engineering a Safer World (2012)”の中で提唱

- 複数の法論
- システムプロセス

プロセス

システム工学(例  
安全性ガイド設計)

ツール(手法)

事故/イベント分析

組織的/文化的リスク

STAMP/STPAにセキュリティの要素を導入を試みたものとしてSTPA-Secなどがある

情報処理学会CSS2017 3C3-2:「安全解析手法

STAMP/STPAに対するセキュリティ視点からの脅威分析の拡張提案」

○金子 朋子(情報処理推進機構), 高橋 雄志(東京電機大学), 大久保 隆夫(情報セキュリティ大学院大学), 勅使河原 可海(東京電機大学), 佐々木 良一(東京電機大学)

IPA作成資料

# STPA-Secの実施手順

## STPA分析手順

**Step 0 : (前準備1)**  
Accident、Hazard、  
安全制約の識別

**Step 0 : (前準備2)**  
Control Structureの  
構築

**Step 1 : UCA (Unsafe  
Control Action) の抽出**

**Step 2 : HCF (Hazard  
Causal factor) の特定**

**最終Step :**  
対策検討・まとめ

## STPA-Secの分析内容 (赤字がSTPAへの追加部分)

対象とする**Accident** (望ましくない事象)、**Hazard**  
(Accidentが潜在している状態) を定義し、Hazardを  
制御するためのシステム上の**安全制約**を識別する

**セキュアでない状態も考慮して**安全制約の実現に関係する  
**コンポーネント** (サブシステム、機器、組織等)、及び  
コンポーネント間の**相互作用** (指示、フィードバック  
データ) を分析し、**Control Structure**を構築する

**情報のライフサイクルを利用したハザードのコントロール  
アクションを追跡したうえで**Control Structureから  
安全制約の実行に必要な指示(Control Action)に**4つの  
ガイドワード**を適用して、ハザードにつながる**非安全な  
Control Action (UCA)** を抽出する

UCA毎に、関係する**Control Loop Diagram**を抽出し、  
**ガイドワード**を適用して**ハザード要因 (HCF)** を特定する

- **セキュアでないコントロールアクションを導くシナリオを識別する**
- **D4チャートでよりクリティカルなセキュリティシナリオを描く**
- **コントロール戦略に用いるセキュリティシナリオを検討する**

**非安全/セキュアでないシナリオを除去、軽減するための  
新しい要求、コントロール、設計を開発**

**STEP2に脅威分析を  
追加**

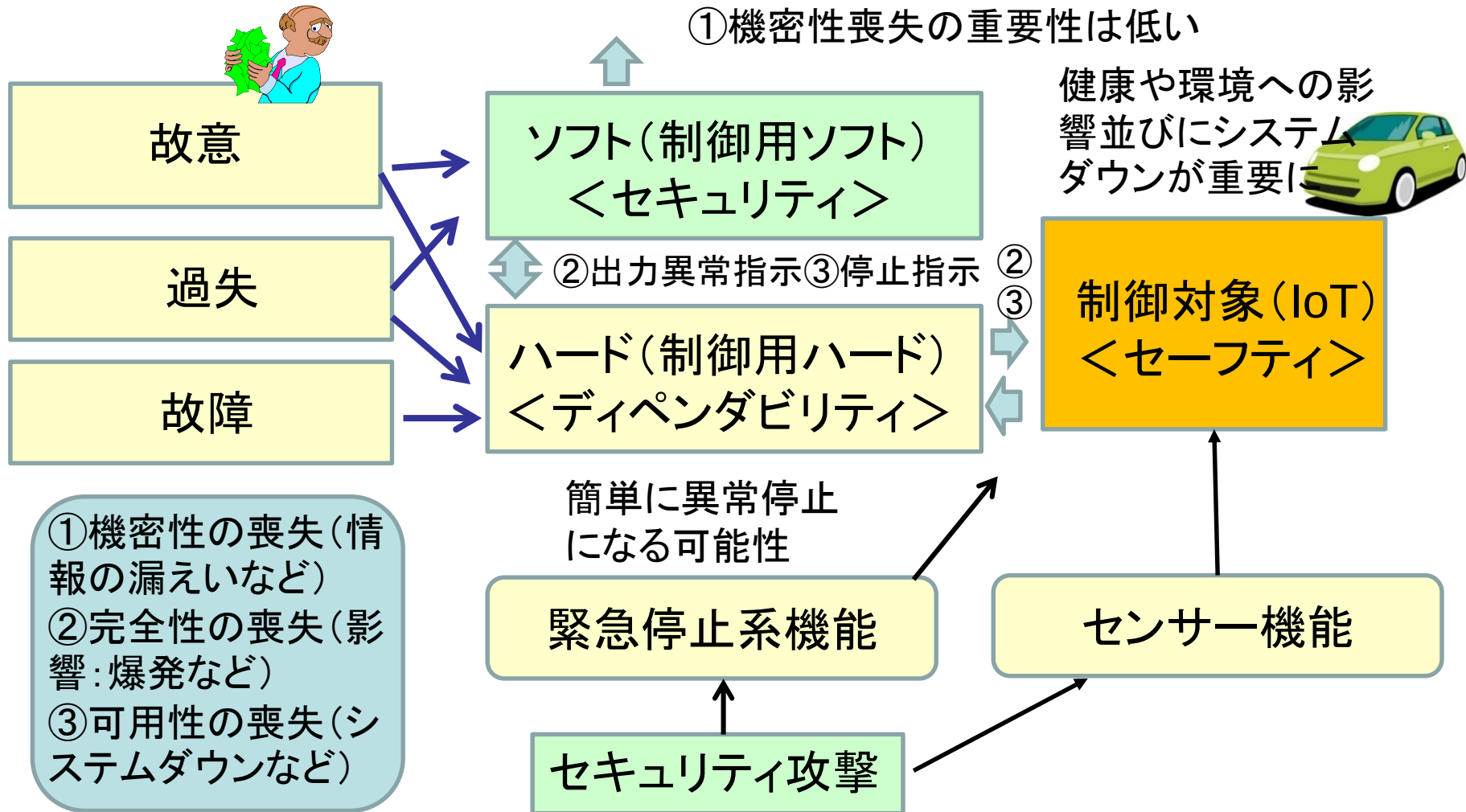
↓  
**マイクロソフトの  
脅威モデルSTRIDEと  
脅威分類Threat Treeを  
ヒントワードとして利用**

↓  
**セキュリティ誘発要因  
の洗い出しと対策立案  
が**

**網羅的にできる**

↓  
**適切な脅威シナリオの  
作成を支援**

# IoTのセキュリティとセーフティ



# IoTを含むシステムのリスク評価の特徴

## 1. ITシステムのリスク評価:

情報のCIAからなるSecurityを中心

IoTを含む場合は制御対象のリスク評価:

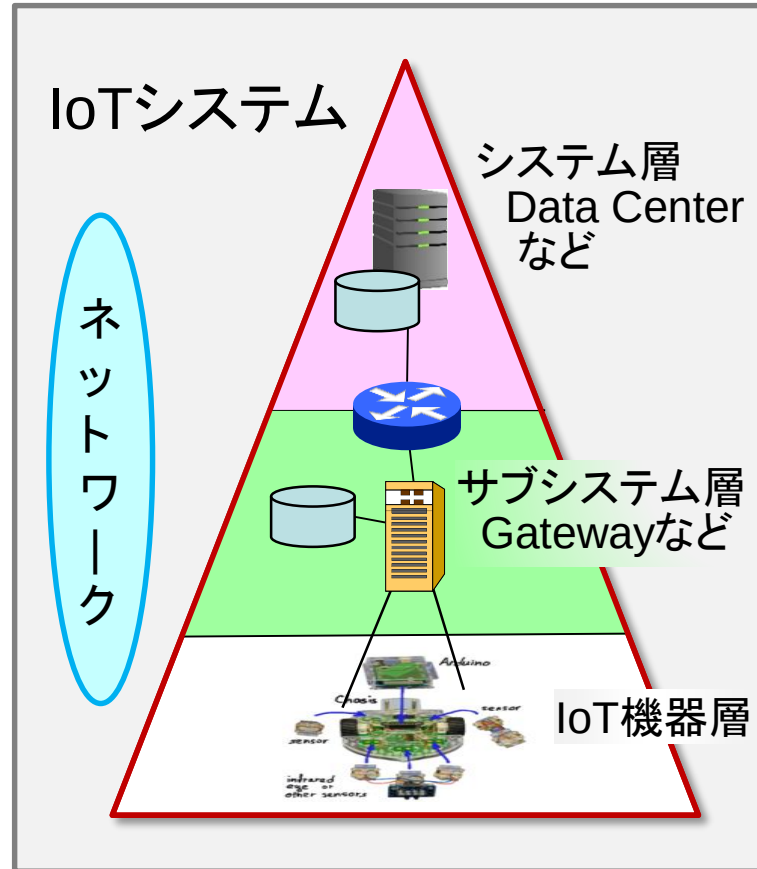
Safetyを主にしSecurityを従にする評価が必要に

2. IoTの種類によっては、センサー系の異常や制御系の異常への対処も重要になる

3. 対策効果の評価まで行う場合は、いろいろなレイヤーでの対策を考慮すべき



# IoTの階層別のセキュリティ対策



＜対象によってセキュリティ対策が大幅に異なる＞

既存のIoT機器

セキュア  
ゲートウ  
エイ

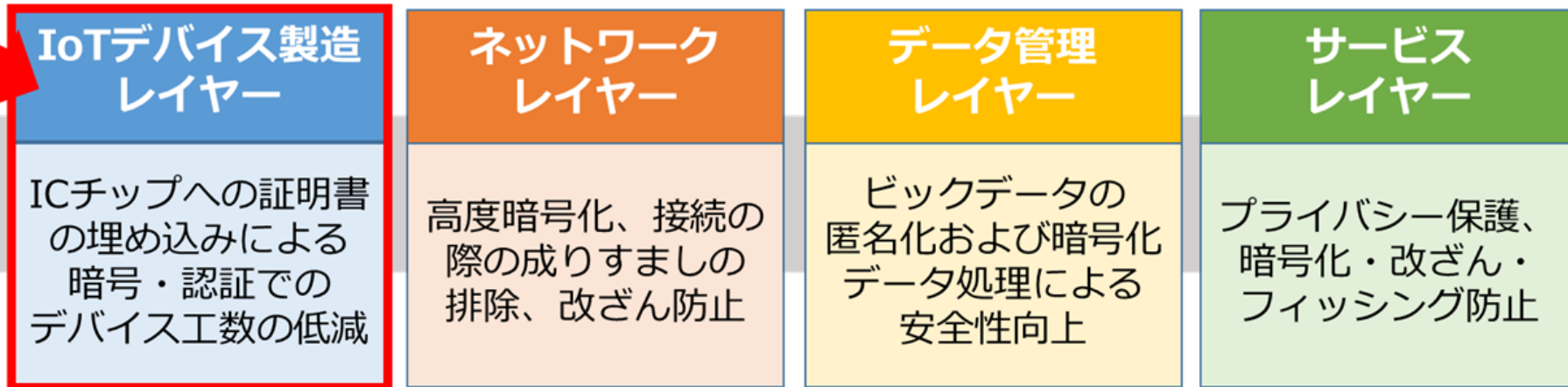
認証  
チップ

種々の対  
策の適切  
な組み合  
わせ

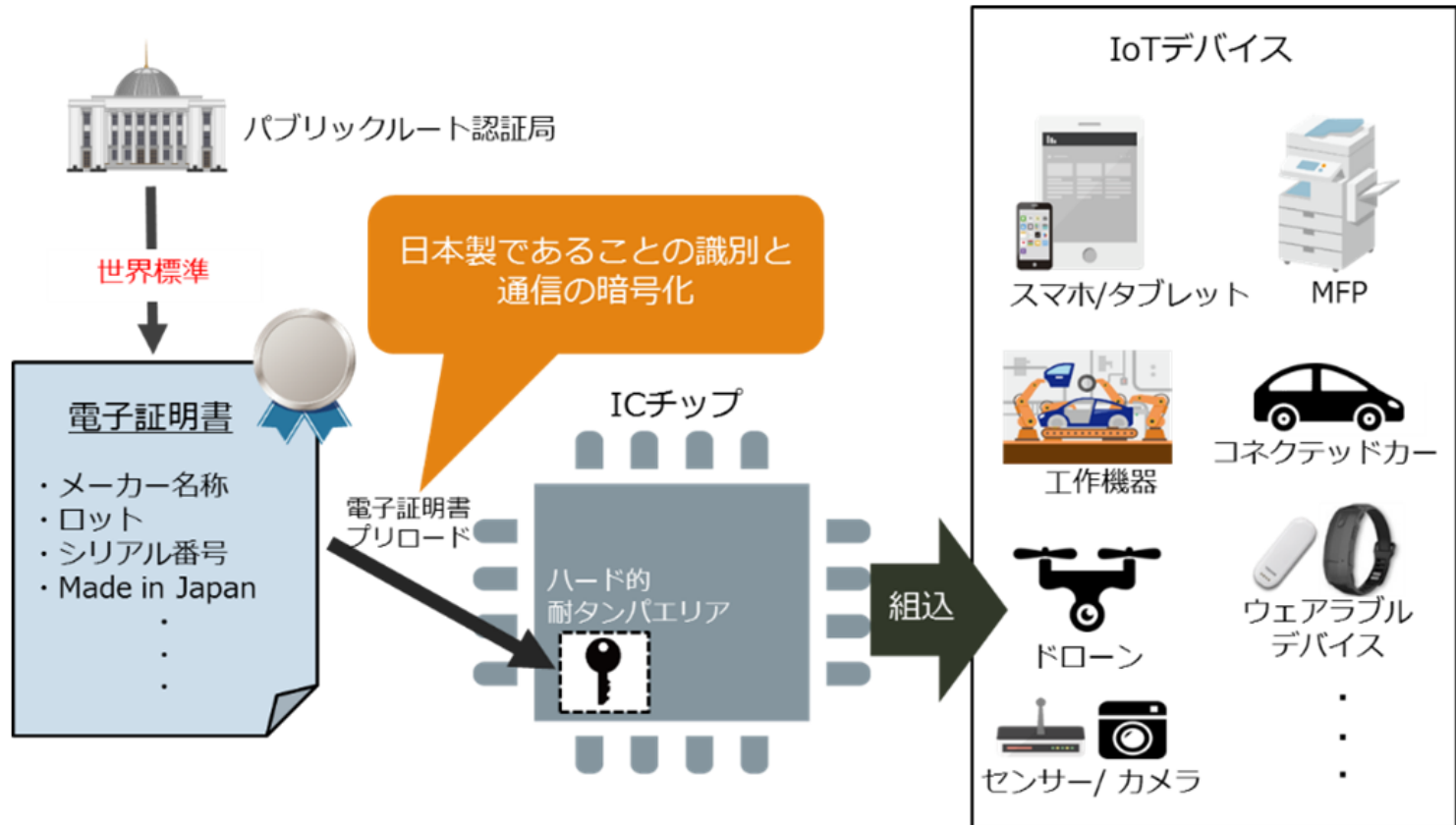
新規中小規模 IoTシステム    新規大規模規模 IoTシステム

# レイヤー別ガイドラインの策定

## ●レイヤーに合わせたセキュリティガイドラインの策定



# IoT機器層向け対策



# 多重リスクコミュニケーター(MRC)ベースの方法

## <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. 多くの関係者(経営者・顧客・従業員など)が存在⇒多くの関係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制約条件とし、残存リスク等を最小化する対策組み合わせ問題として定式化

②関係者の合意が得られるまで制約条件値などの値を変えつつ最適化エンジンを用い求解



専門家

対策案

①②③④

定式化  
結果

多重リスク  
コミュニケー  
ターMRC

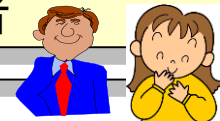
最適解  
対策案  
①③の  
組合せ

END

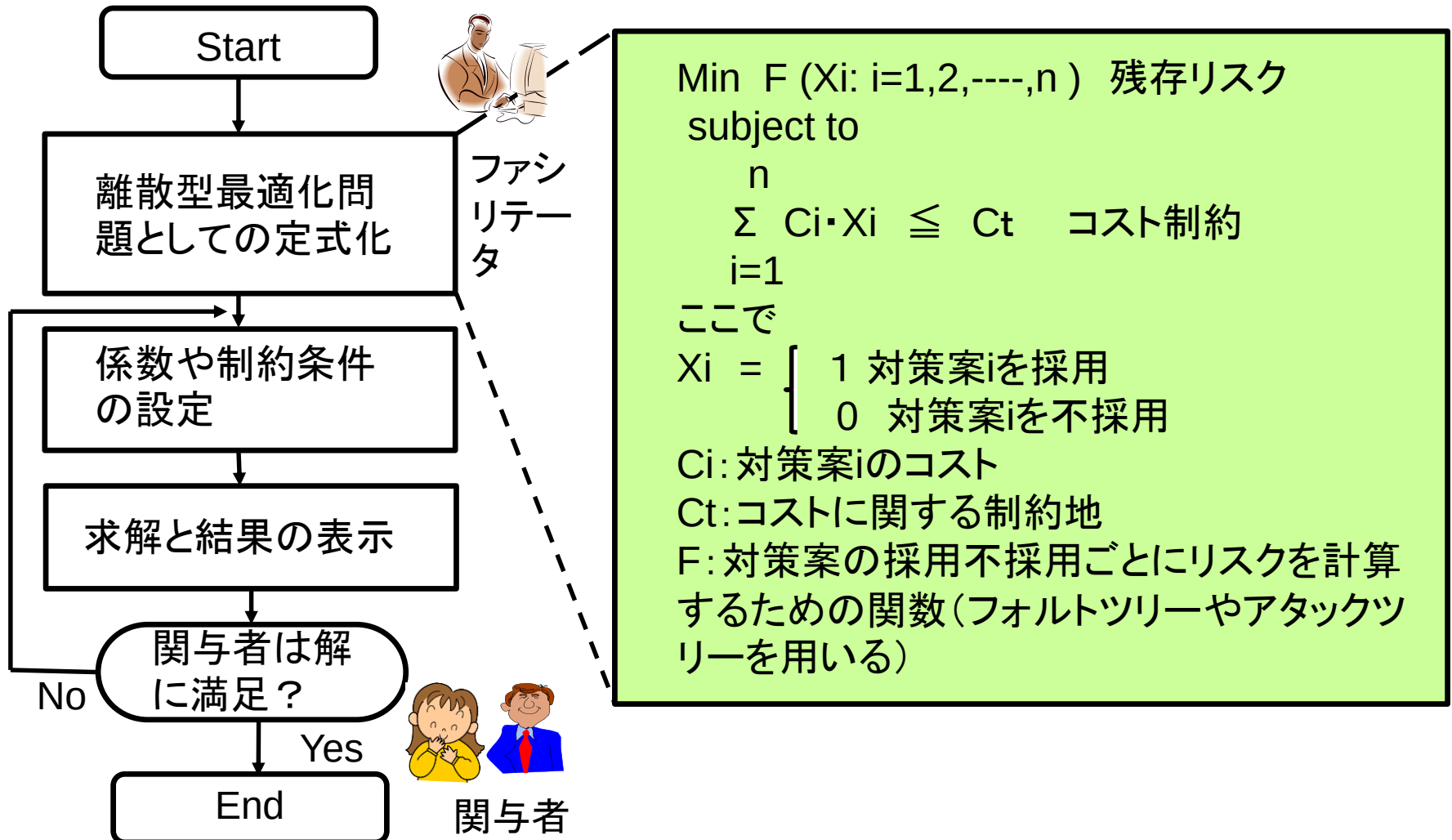
満足

制約条件などの変更

ファシリテーター 関係者

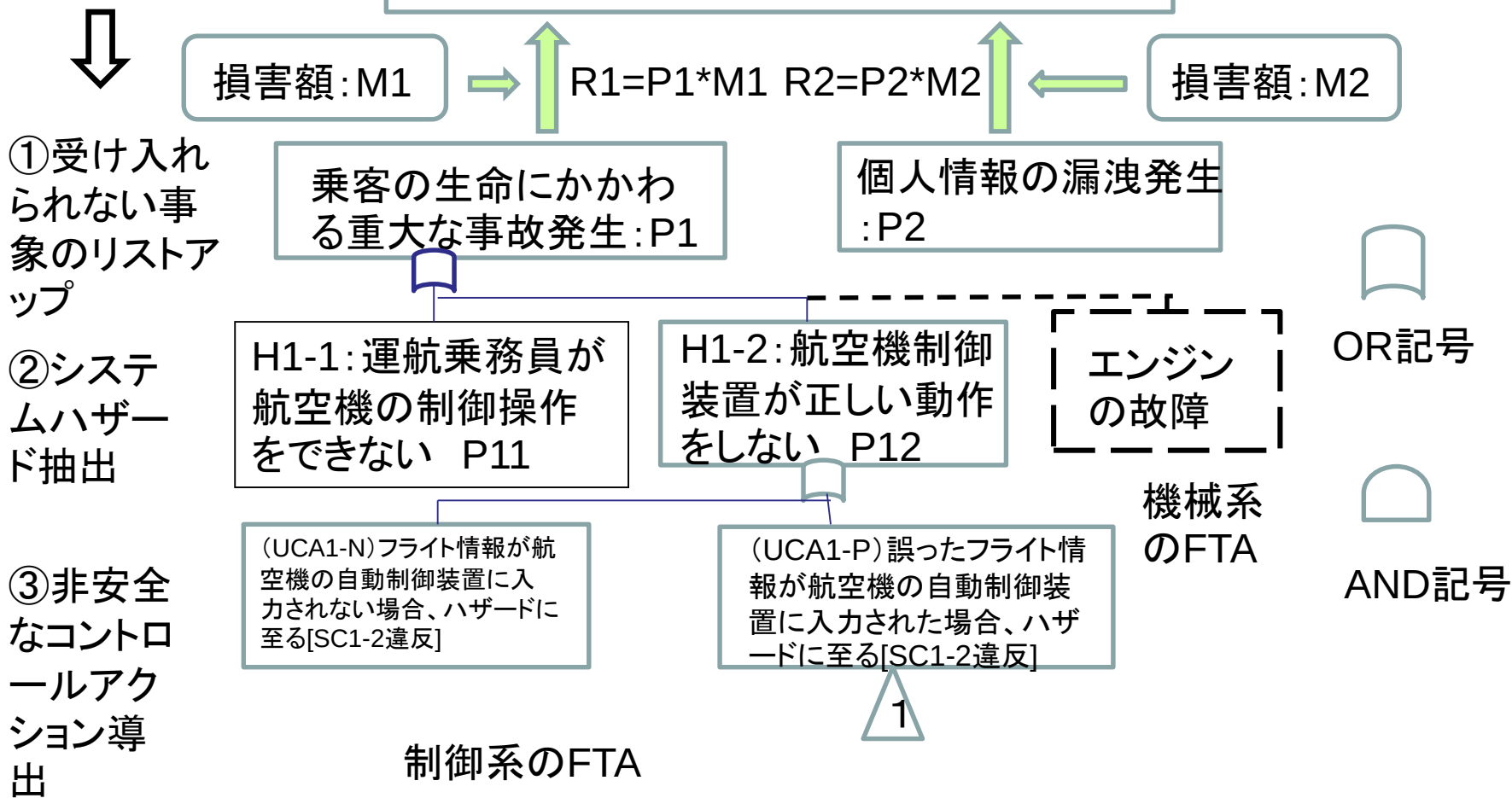


# 多重リスクコミュニケーター(MRC)の手順



# 残存リスクの計算方法案＜定量的（１）＞

STPAの方式



# 残存リスクの計算方法案＜定量的（2）＞

## ④アタックツリー的方式を利用

1

これらのリストアップに  
STPA-Secで提案の方法  
を利用

航空機制御装置から  
の情報を改ざんする  
ことによる事故

航空会社の装置から  
の情報が改ざんされ  
ている（実際よりも低  
く飛ぶよう改ざん）

航空会社—航空機制  
御装置間の情報を改  
ざんする（実際よりも  
低く飛ぶよう改ざん）

航空機制御装置からの  
情報を改ざんする（実際  
よりも高いところを飛ん  
でいると改ざん）

信号が正しいと思  
い航空会社の装置  
が高度をもっと下げ  
るよう指示

航空乗務員が気  
付かない

## ＜対策案＞

改ざん検知符号をつ  
けるX1（効果：q1）

対策3 X3（効果q3）

# アプローチ方法案＜半定量的＞

| 受け入れられない損失／アクシデント(P1) | システムハザード                  | 非安全なコントロールアクション                    | 脅威  |                     |    | トータルリスク(p3 = p1x p2) | 考慮対象 | 対策案       |          |         |   |
|-----------------------|---------------------------|------------------------------------|-----|---------------------|----|----------------------|------|-----------|----------|---------|---|
|                       |                           |                                    | 部位  | 記述                  | P2 |                      |      | 1         |          |         | 2 |
|                       |                           |                                    |     |                     |    |                      |      | 効果q1      | P3Xq     | コスト     |   |
| 乗客の生命にかかわる重大な事故発生     | H1-1: 運航乗務員が航空機の制御操作をできない | フライト情報が航空機の自動制御装置に入力されない場合、ハザードに至る | 乗務員 | コンピュータに対し、他のユーザーを装う | 3  | 1                    | ①    | リスクが30%低減 | 1<br>4.5 | 100万円   |   |
|                       |                           |                                    |     |                     |    | 5                    |      | ②         | —        | —       |   |
|                       | H1-2: 航空機制御装置が正しい動作をしない   |                                    |     |                     |    |                      |      | —         | —        |         |   |
|                       |                           |                                    |     |                     |    | 10                   | ③    | リスクが10%低減 | 1        | (100万円) |   |
| 5                     |                           |                                    |     |                     |    |                      |      |           |          |         |   |
| 個人情報の漏洩発生             |                           |                                    |     |                     |    |                      |      |           |          |         |   |
| 3                     |                           |                                    |     |                     |    |                      |      |           |          |         |   |
|                       |                           |                                    |     |                     |    |                      |      |           |          |         |   |

| 結果表       |    |    |    |
|-----------|----|----|----|
| コスト<br>効果 | 大  | 中  | 小  |
| 小         |    | 対策 |    |
| 中         | 対策 | 3  | 対策 |
| 大         | 2  |    | 1  |

結果表

| 効果 \ コスト | 大  | 中  | 小  |
|----------|----|----|----|
| 小        |    | 対策 |    |
| 中        | 対策 | 3  | 対策 |
| 大        | 2  |    | 1  |

定量化がむづかしい場合にはこのような半定量的方法も考えられる

それぞれ5段階の方がよさそう

# 目次

---

1. はじめに
2. IoTのセキュリティが重要になった背景
3. IoTへの攻撃
4. IoTを含むシステムへのリスク評価法の考察
5. 今後の方向



# おわりに

---

1. IoTシステムのセキュリティ対策は今後ますます重要に
2. IoTシステムのリスク評価・リスクコミュニケーションも大切に
3. IoTシステムは複雑で、しかもセーフティとセキュリティを同時に考えていく必要があり対応は簡単ではない
4. 提案方式を適用しつつ改良を図っていく  
(作業量を減らすための検討も必要)



# ITリスク参考文献(1)

---

- 1) 佐々木良一「ITリスクの考え方」岩波新書、2008
- 2) 佐々木良一他「多重リスクコミュニケーターの開発と適用」情報処理学会論文誌、Vol49, No9, 2008年9月号
- 3) 谷山 充洋、佐々木良一 他「多重リスクコミュニケーターの企業向け個人情報漏洩問題への適用」日本セキュリティマネジメント学会誌、Vol.23, No.2、pp34-51
- 4) 谷山 充洋、佐々木良一「多重リスクコミュニケーターの教育方法の提案と分析」日本セキュリティマネジメント学会誌、VOL.23, No.2、pp52-64
- 5) 土方広夢、佐々木良一他「デジタル・フォレンジクスを考慮した個人情報漏洩対策に関する合意形成のための多重リスクコミュニケーターの適用」日本セキュリティマネジメント学会誌 26巻第1号2012年5月pp3-14
- 6) 佐々木良一「ITリスク学の動向・技術と社会と安全と」IEICE Fundamental Review Vol.4 No.3(電子通信学会)



# ITリスク参考文献(2)

---

- 7) 佐々木良一他「ITリスク対策に関する社会的合意形成支援システムSocial-MRCの開発構想」情報処理学会論文誌VOL.52,No.9、pp 2562-2574
- 8) Ryoichi Sasaki et al., “ Proposal for Social-MRC: Social Consensus Formation Support System Concerning IT Risk Countermeasures”, International Journal of Information Processing and Management (2012) Vol.2, No.2 pp48-58
- 9) Ryoichi Sasaki, “ Consideration on Risk Communication for IT Systems and Development of Support Systems” Journal of Information Processing Vo.20(2012)-4, pp814-822 (Invited Paper)
- 10) 大河原優、佐々木良一他「ITリスク対策に関する社会的合意形成支援システムSocial-MRCの情報フィルタリング問題への試適用と考察」日本セキュリティマネジメント学会誌 25巻第3号2012年1月pp15-23
- 11) 佐々木良一編著「ITリスク学 情報セキュリティを超えて」共立出版, 2013



