IoT時代の
リスク評価技術の研究

東京電機大学未来科学部教授
サイバーセキュリティ研究所所長
佐々木良一
sasaki@im.dendai.ac.jp

目次

最近の動向とリスク評価への要求

＜最近の動向＞

サイバー攻撃が高度化

セキュリティ対策が高コスト化

IoTが普及

＜リスク評価への要求＞

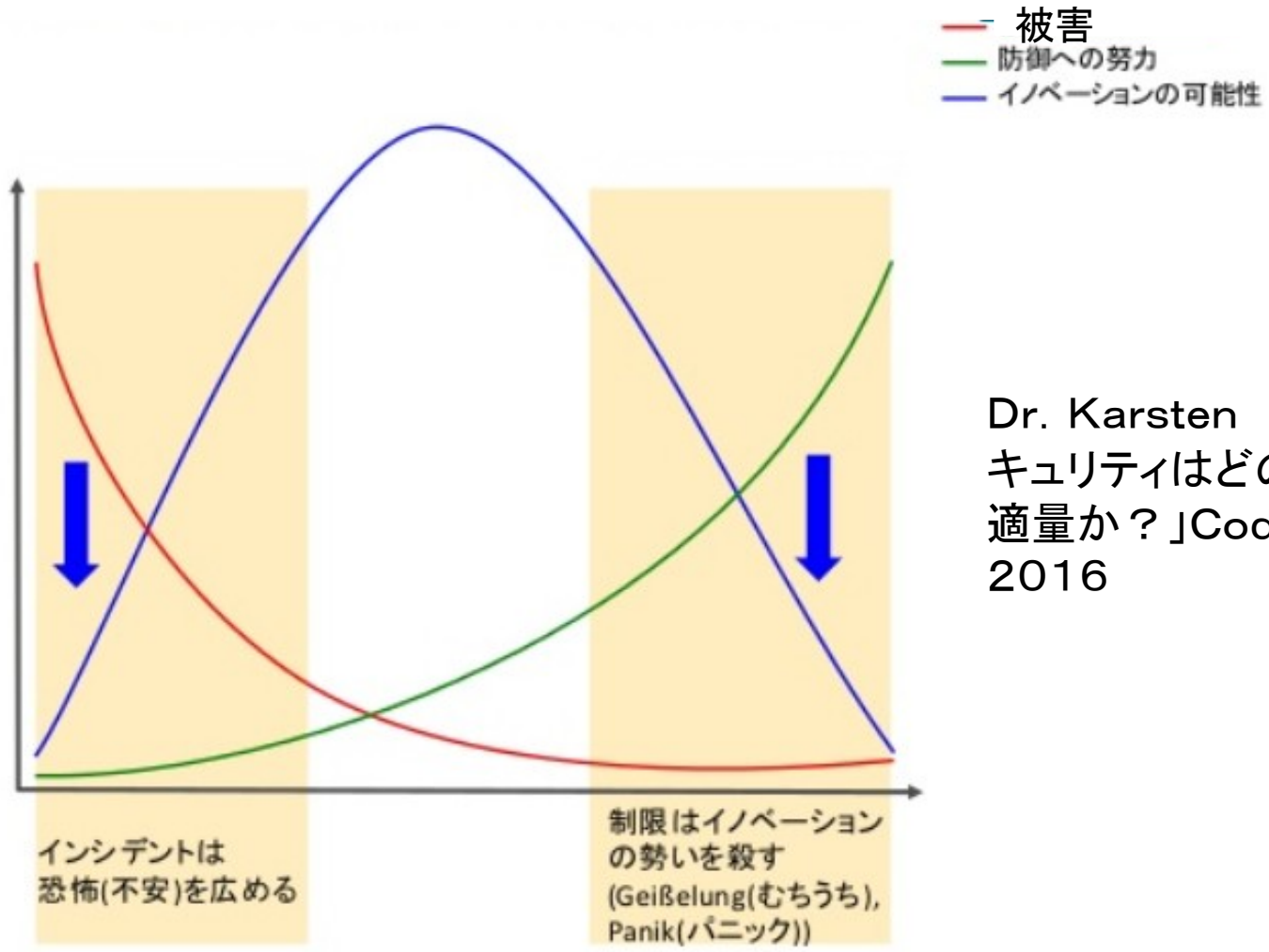
どこまで対策すべきか明確にしてほしい

多段にわたる攻撃への評価方法が大切に

経営者のリスク評価への参加が不可欠に

制御対象であるIoTを含めたリスク分析が重要に

最適なリスク対策額



Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

アプローチ法

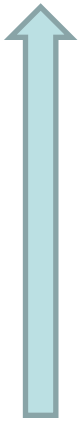
＜従来＞
(i) 脅威を重視したアプローチ
(ii)資産を重視したアプローチ
(iii) 脆弱性を重視したアプローチ

＜今後＞
リスクを重視したアプローチ
リスク＝資産X脆弱性X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

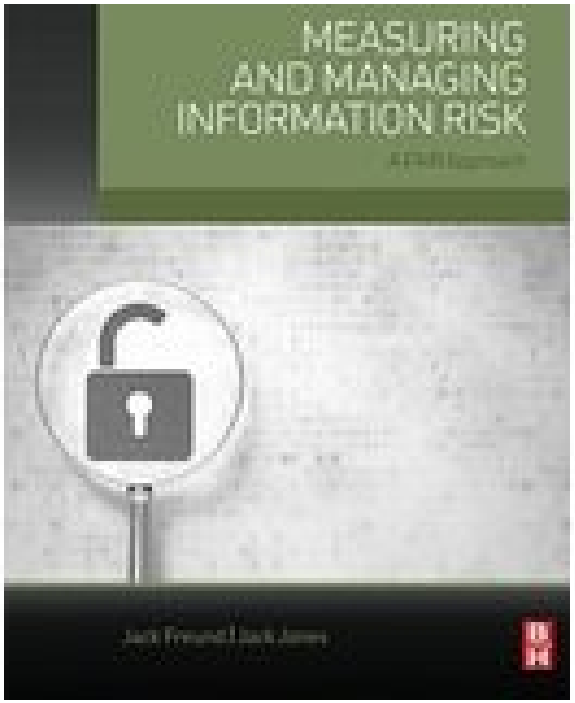


FIPS SP 800-30を参考に作成

FAIRアプローチ

Jack Freund, Jack Jones
“Measuring and Managing Information Risk　A FAIR Approach”
Elsevier, 2015

FAIR：Factor Analysis of Information Risk



「定量的リスク分析を積極的に扱い発生確率の不確実性を考慮し、モンテカルロ法を用いてリスクの分布を求めるような方法も提案されている。」

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 リスク学 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 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

目次

多重リスクコミュニケータ（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関与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

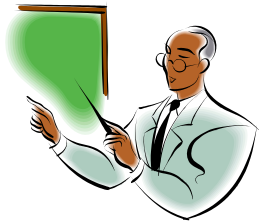
ファシリテータ　関与者

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

（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

2．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)

最近のITのリスク評価への要求

＜最近の動向＞

サイバー攻撃が高度化

セキュリティ対策が高コスト化

IoTが普及

＜リスク評価への要求＞

どこまで対策すべきか明確にしてほしい

多段にわたる攻撃への評価方法が大切に

経営者のリスク評価への参加が不可欠に

制御対象であるIoTを含めたリスク評価が重要に

目次

EDC法の開発

EDC法

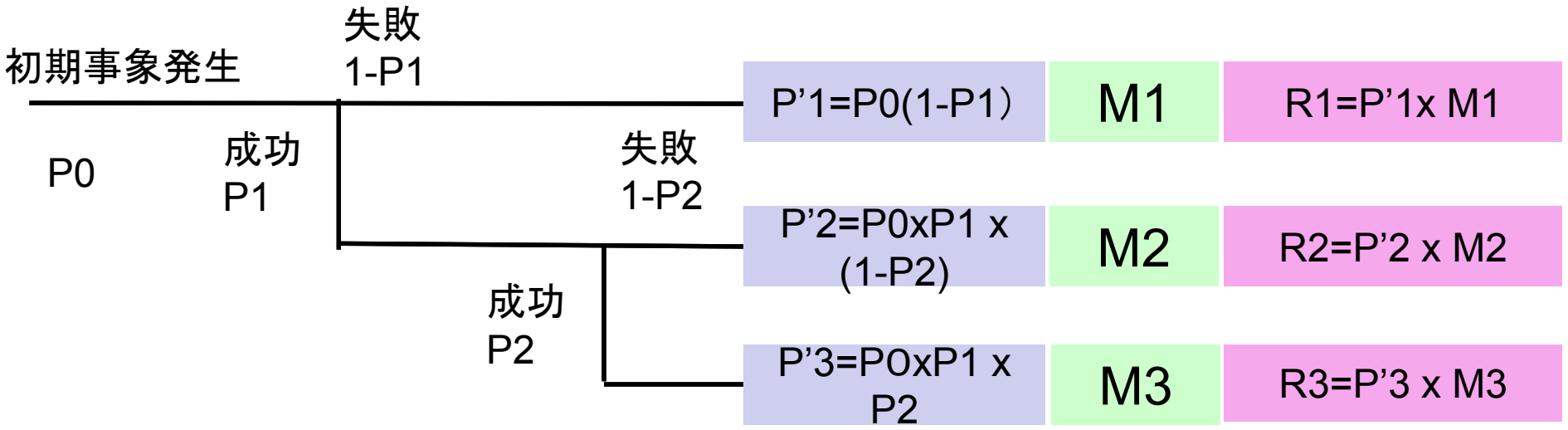
イベントツリー分析法 ＋ ディフェンスツリー分析法

EDC法： Event Tree and Defense Tree Combined Method
東京電機大学サイバーセキュリティ研究所での研究の一環

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

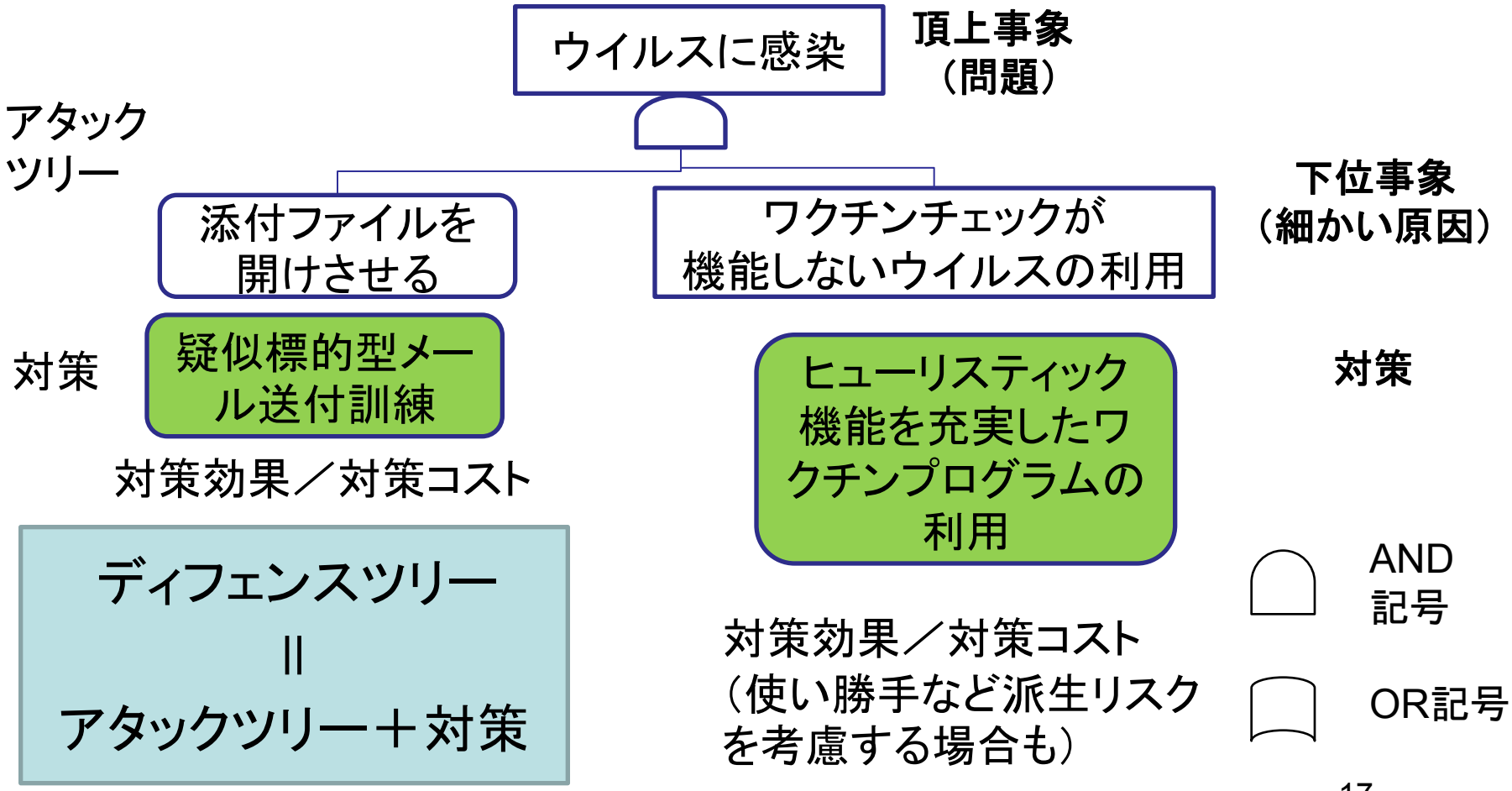
ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）



RT=R1+R2+R3

ディフェンスツリー分析

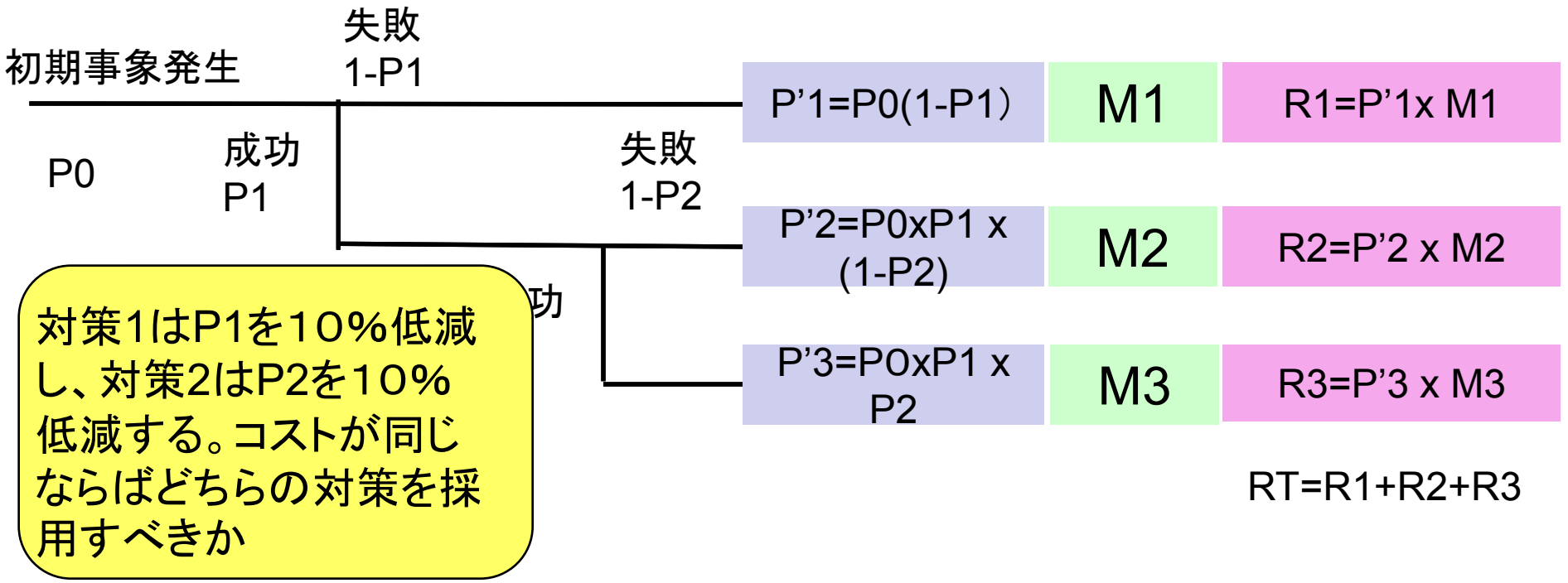
- 攻撃に対しトップダウンにその要因を分析する
  アタックツリー分析に対策を加えたもの



イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）



イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
初期事象発生	失敗 1-P1	0.8	0円	0円
P0 1.0	成功 P1			
	0.2	0.16	500万円	80万円
	失敗 1-P2			
	成功 P2	0.04	1億円	400万円
	0.2			

トータルリスク= 480万円

対策1はP1を10%低減し、対策2はP2を10%低減する。コストが同じならばどちらの対策を採用すべきか

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
失敗 1-P1		0.856	0円	0円
成功 P1	失敗 1-P2	0.144	500万円	72万円
	成功 P2	0.036	1億円	360万円

初期事象発生

P0
1.0

0.2X0.9

0.2

対策1を実施した場合（対策1はP1を10%低減）

トータルリスク=
432万円
（低減効果　48万円）

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

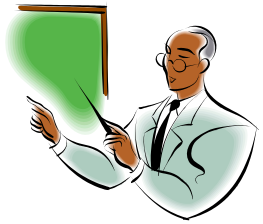
ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
初期事象発生	失敗 1-P1	0.8	0円	0円
P0 1.0	成功 P1			
	0.2	失敗 1-P2	0.164	500万円	82万円
		成功 P2	0.036	1億円	360万円
		0.2X0.9			

対策2を実施した場合（対策2はP2を10%低減）

（対策1の低減効果は48万円）

トータルリスク=
442万円
（対策2の低減効果38万円）

EDC法の実適用



（1）東京電機大学の次期セキュリティ対策

（2）守るべきもの：学生の成績情報

1人当たり賠償額：5500円（JNSA方式）

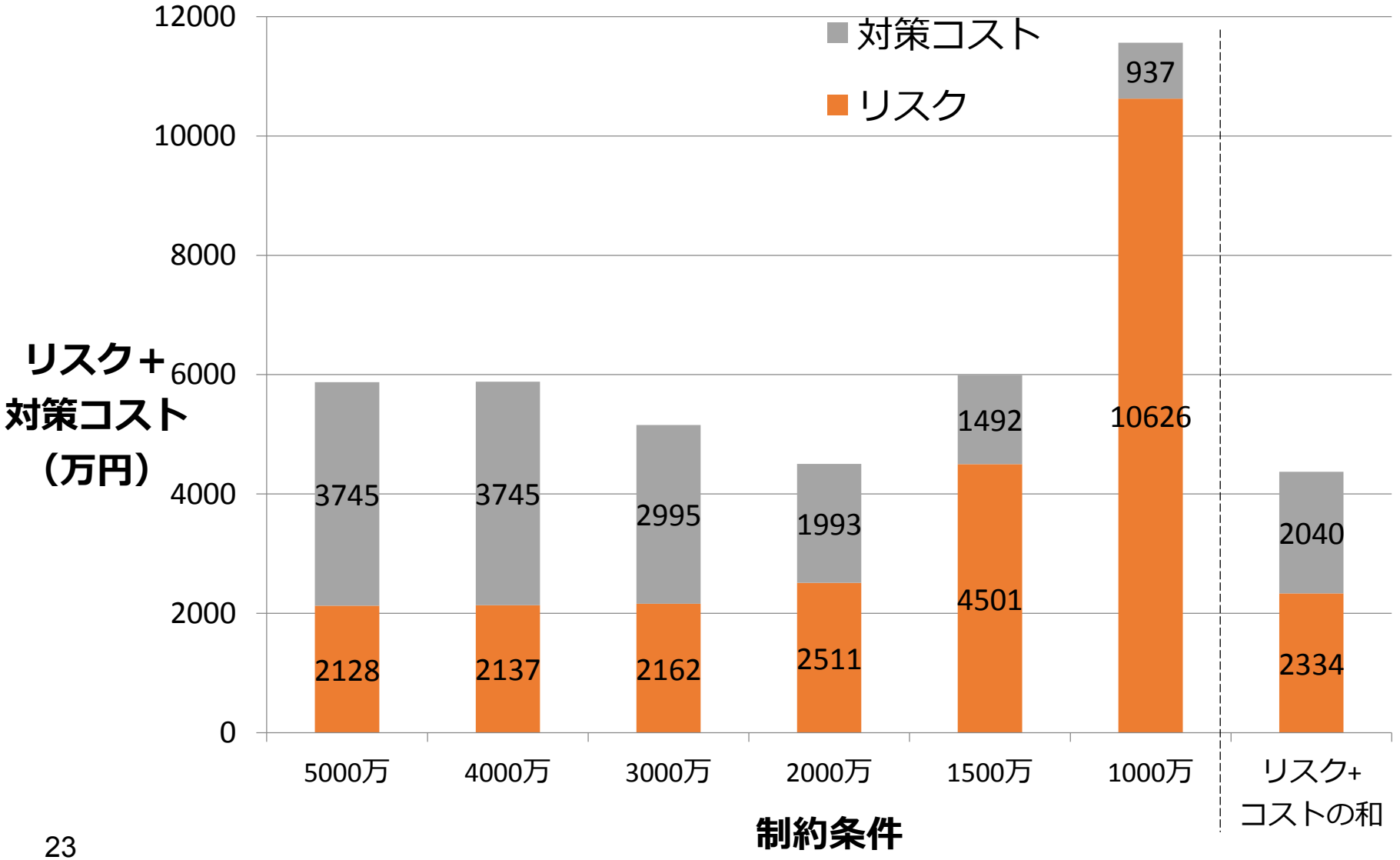
サーバ内（全学学生数：1万人）

教員のPC内（一学科あたり　500人）

（3）対象攻撃：標的型メール攻撃

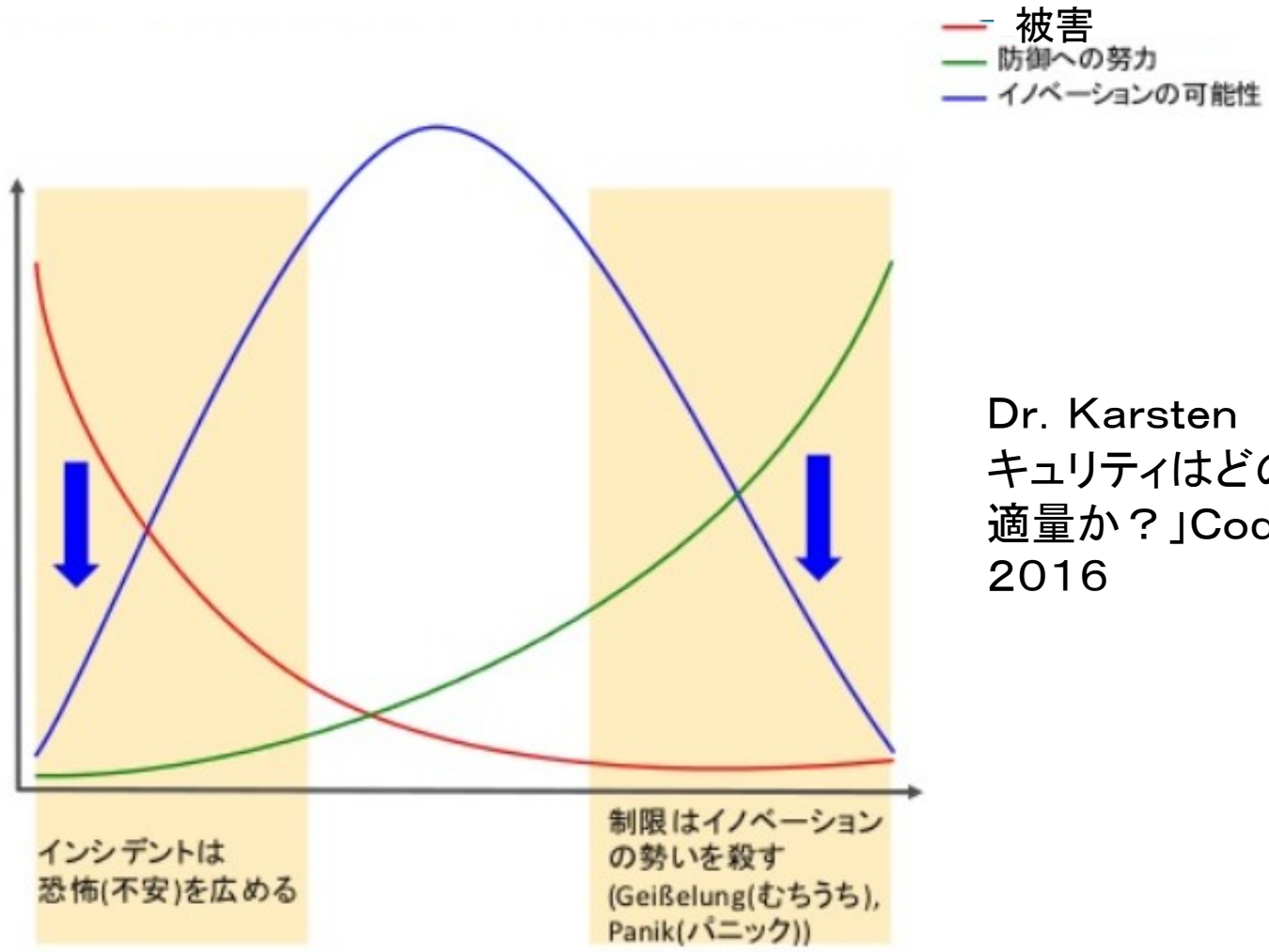
（4）対策案数：約30個（それぞれにコストや直接的効果を設定）

最適解求解結果


対策コスト
リスク
12000
10000
8000
6000
4000
2000
0
リスク＋
対策コスト
（万円）
3745
3745
2995
1993
1492
937
2128
2137
2162
2511
4501
10626
2040
2334
5000万
4000万
3000万
2000万
1500万
1000万
リスク+
コストの和
制約条件

（最小値）

最適なリスク対策額



Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

結論

- 総合リスク値＋対策コストが最小となる対策

メールフィルタの導入（入口）
製品Aによる監視（入口―内部）
標的型攻撃対策訓練の実施（入口）
製品Bによる監視（入口―内部）
PCやサーバのパッチの最新化（内部）
プロキシを経由しない通信の遮断（出口）
プロキシによる監視（出口）
二要素認証（内部）

総合リスク値	2005万円/年
対策コスト	2617万円/年

目次

最近のITのリスク評価への要求

＜最近の動向＞

サイバー攻撃が高度化

セキュリティ対策が高コスト化

IoTが普及

＜リスク評価への要求＞

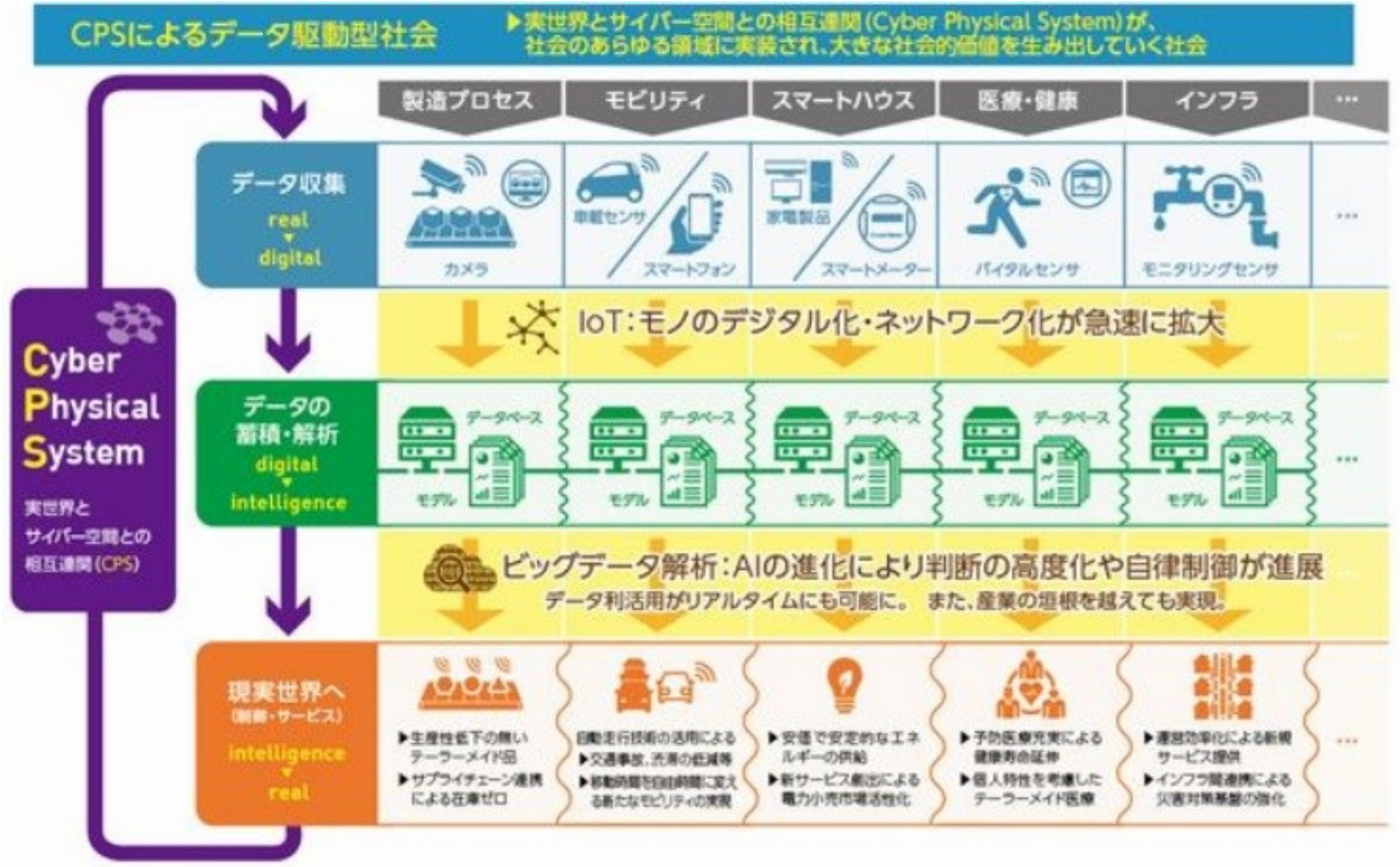
どこまで対策すべきか明確にしてほしい

多段にわたる攻撃への評価方法が大切に

経営者のリスク評価への参加が不可欠に

制御対象であるIoTを含めたリスク評価が重要に

CPS/IoT時代の到来



http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

主要なIoT装置

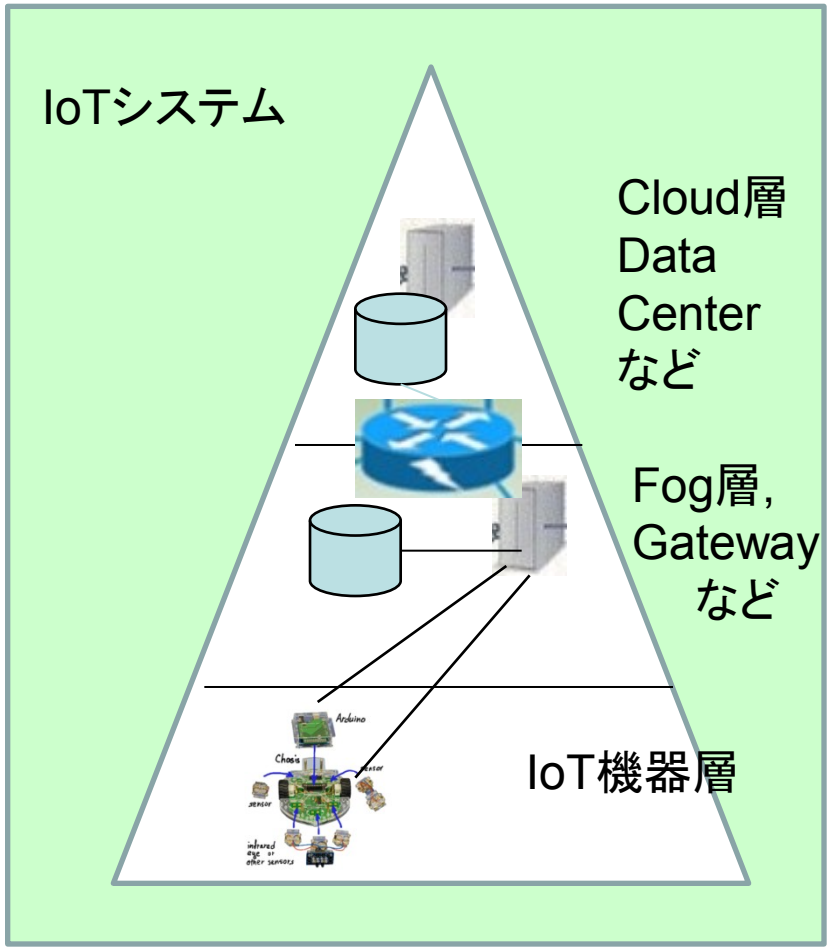
- 制御システム
- 自動車
- センサーネット
  スマートメータなど
- 組み込み系
  情報家電
  防犯カメラ
  複合機
  医療機器など

IoT 特有の性質

（性質１）脅威の影響範囲・影響度合いが大きいこと
（性質２）IoT 機器のライフサイクルが長いこと
（性質３）IoT 機器に対する監視が行き届きにくいこと
（性質４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること
（性質５）IoT 機器の機能・性能が限られていること
（性質６）開発者が想定していなかった接続が行われる可能性があること

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

IoTの階層別のセキュリティ対策



＜セキュリティ対策＞

既存
のIoT
機器

新規中小規模
IoTシステム

新規大規模規模
IoTシステム

ITのセキュリティ

故意

過失

故障

①機密性喪失が重点問題

ソフト
＜セキュリティ＞

コンピュータハード
＜ディペンダビリティ＞

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

故意

過失

故障

①機密性喪失の重要性は低い

ソフト（制御用ソフト）
＜セキュリティ＞

②出力異常指示③停止指示

ハード（制御用ハード）
＜ディペンダビリティ＞

②
③

制御対象（IoT）
＜セーフティ＞

健康や環境への影響並びにシステムダウンが重要に

簡単に異常停止になる可能性

セーフティ機能

セキュリティ攻撃

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）

研究の進め方

	ITシステム	IoTを含むシステム	
	Security	Safety	Safety& Security
ユーザの運用段階	既開発 ①多重リスクコミュニケータ ②EDC法など	調査 ①シナリオ法 ②STAMP法 ＆STPA法	新技法の提案 （例えば改良型STAMP法あるいはまったく違った方法）
プロバイダーによる設計段階	調査 ①セキュリティBy デザイン		新技法のS&S By デザインへの組み込み

スマートハウスに対するシナリオ法の適用

リスクのパターン分類

（a）応用ソフトと状況の不具合

シナリオ作成、例えば「留守の間に自動空調アプリが立ち上がり窓を自動的に開け、泥棒が侵入」

（b）応用ソフト間の競合

（b）応用ソフトとユーザ操作の競合

東京大学生研と総務省が協力して実施中の検討会での議論を参考に作成

STAMP法の概要

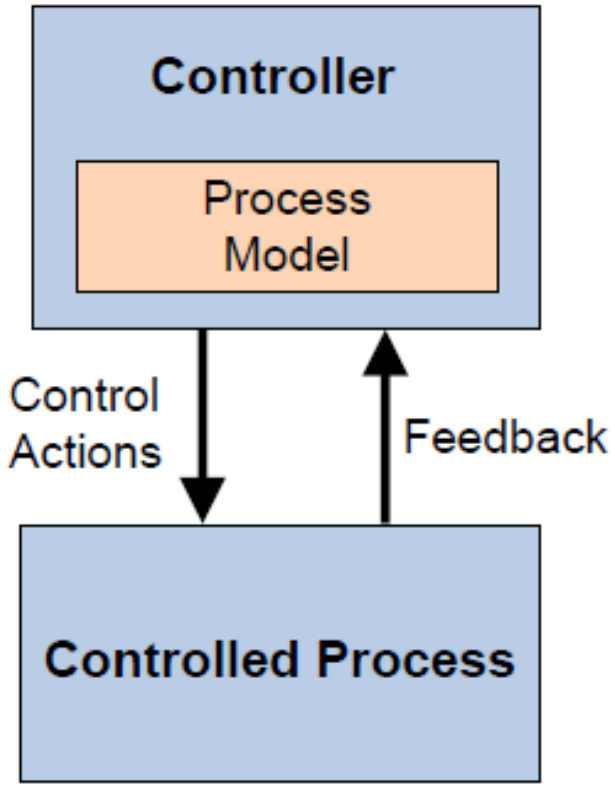
1. MITのNancy G. Leveson教授が提唱
2. 安全解析のパラダイムシフト

   従来手法（FTAなど）：アクシデントは構成機器の故障やオペレーションミスで起きると仮定（ハード対象）

   新たな手法（STAMP法など）：アクシデントは構成要素間の相互作用から創発的に発生すると仮定（コンピュータやIoT対象）

STAMP法：System-Theoretic Accident Model and Process
http://www.ipa.go.jp/sec/reports/20160428.html

Basic STAMP

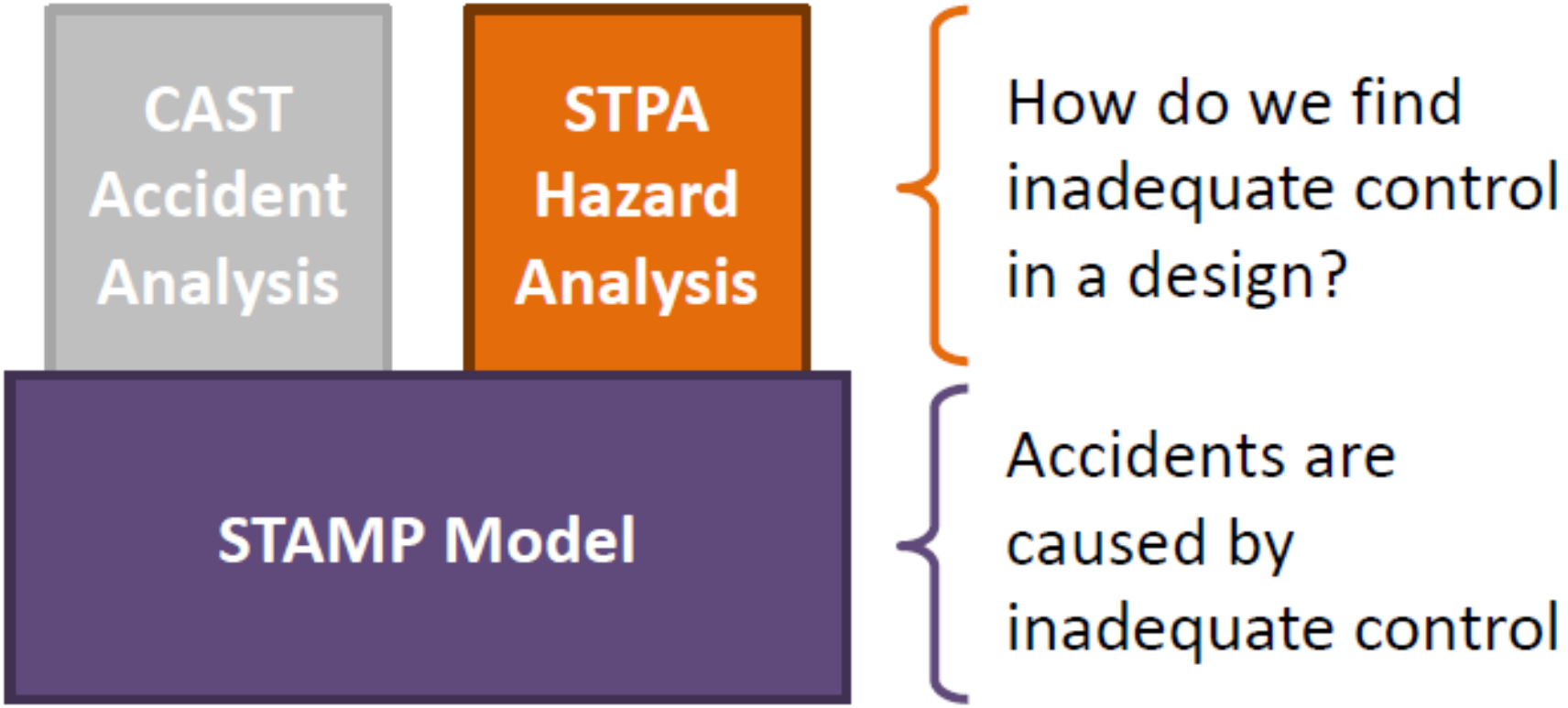


- Controllers use a **process model** to determine control actions
- Unanticipated behavior often occurs when the process model is incorrect
- Four types of **inadequate control actions**:
  1) Control commands are not given
  2) Inadequate commands are given
  3) Potentially correct commands but too early, too late
  4) Control action stops too soon or applied too long

Tends to be a good model of both software and human behavior
Explains software errors, human errors, interaction accidents,..

http://www.ipa.go.jp/files/000056812.pdf

STAMP and STPA



STAMP法：System-Theoretic Accident Model and Process
STPA: System Theoretic Process Analysis

http://www.ipa.go.jp/files/000056812.pdf

目次

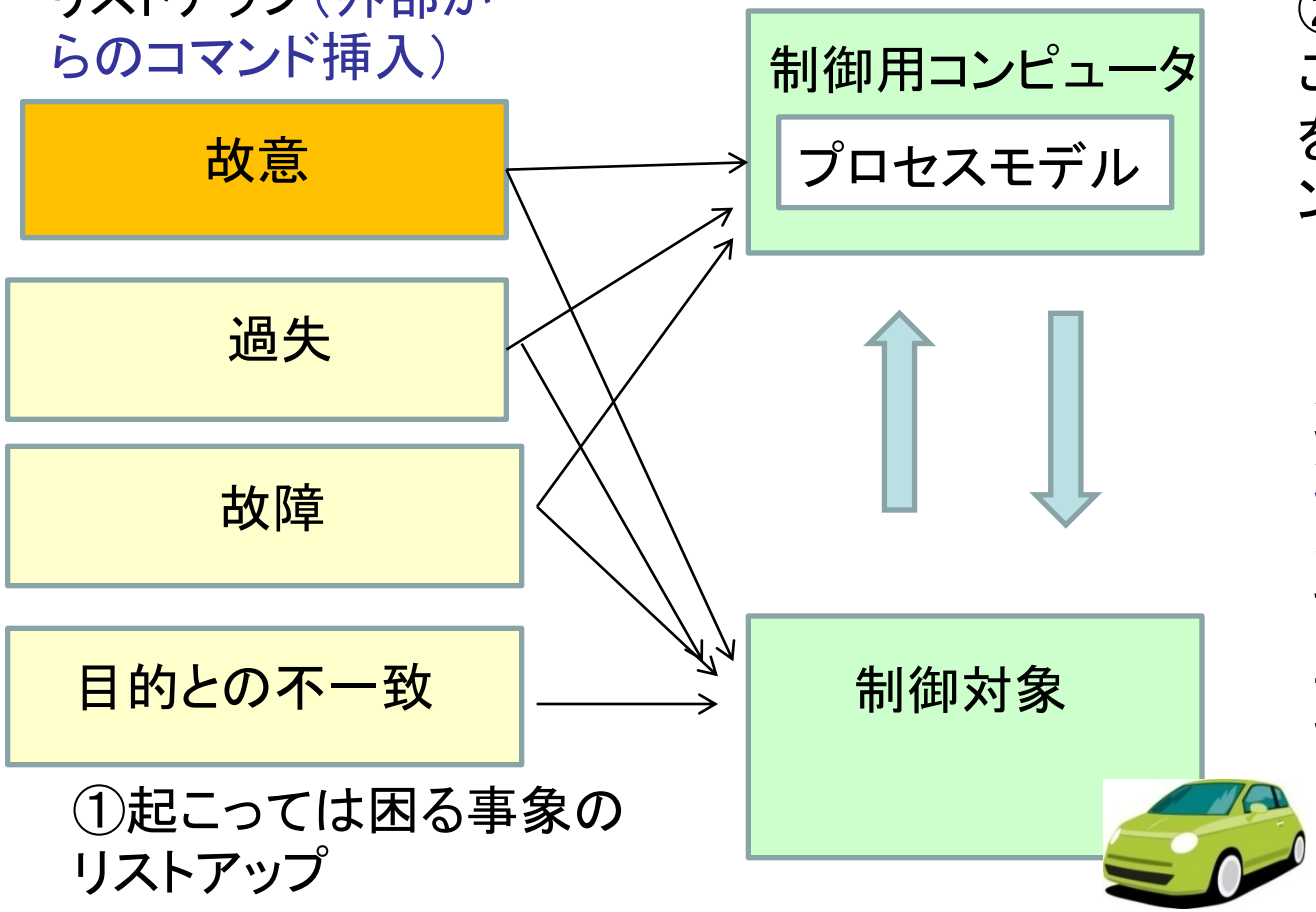
研究の進め方

	ITシステム	IoTを含むシステム	
	Security	Safety	Safety& Security
ユーザの運用段階	既開発 ①多重リスクコミュニケータ ②EDC法など	調査 ①シナリオ法 ②STAMP法 ＆STPA法	新技法の提案 （例えば改良型STAMP法あるいはまったく違った方法）
プロバイダーによる設計段階	調査 ①セキュリティBy デザイン		新技法のS&S By デザインへの組み込み

設計上はセーフティファーストで考え、そこにサイバー攻撃等の影響を追加していくべきか

新技術の候補例

③故意に制御コマンドを出させる攻撃のリストアップ（外部からのコマンド挿入）



①起こっては困る事象のリストアップ
（ハンドルの異常自動操作による事故の発生）

②次の観点から起こっては困る事象をもたらす制御コマンドのリストアップ

1）制御コマンドなし
2）不適切な制御コマンド（ハンドル操作コマンド）
3）早すぎあるいは遅すぎの制御コマンド
4）短すぎたり長すぎたりの制御コマンド

おわりに

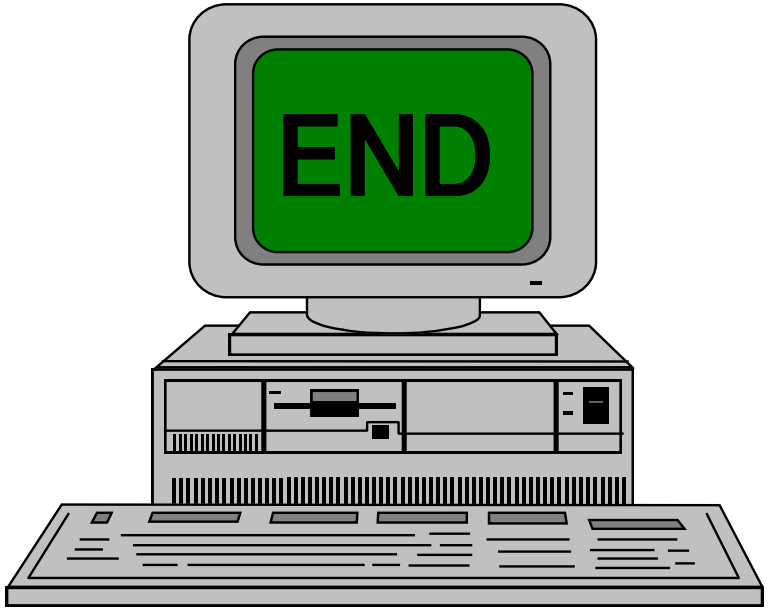
1. IoTシステムのセキュリティ対策は今後ますます重要に

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. 一方、この分野の研究者の数は限られている

5. 共同研究や日本セキュリティ・マネジメント学会ITリスク学研究会を通じた情報交換が大切に


END