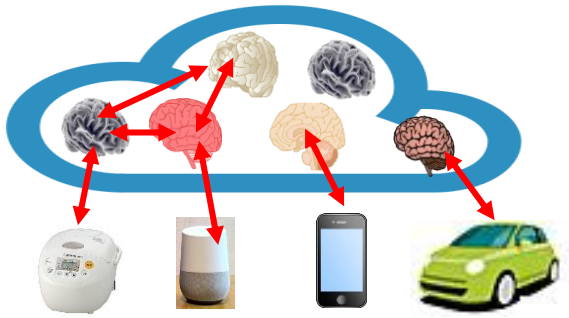
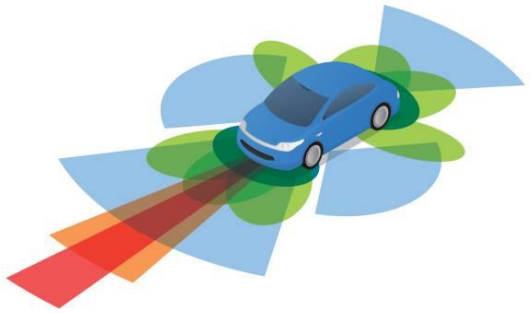
つながることの価値を活かす Safety and Security by Designのアプローチ





名古屋工業大学　社会工学科

橋本芳宏

https://web.manage.nitech.ac.jp/Security

日本機械学会2022年次年会「機械のサイバーセキュリティ ～つながる機械の落とし穴～」

2022年10月12日(月)　富山大学

目次

つながることの価値を活かす
Safety and Security by Designのアプローチ

（前半）つながることの革新性

- IoT, AI, Big Data, DX 時代の変革
- 自動運転と安全＆セキュリティの問題
- 機械のサイバーセキュリティ ～つながる機械の落とし穴～

（後半）システム開発における安全とセキュリティの確保

- サイバー攻撃に対する安全の拠り所
- 開発後の脆弱性管理を考慮した開発プロセス
- SBOMの普及とサイバーセキュリティ管理

IoT, DXの推進技術

- **コンピュータの処理能力**
  1995年から2022年で650万倍（1年かかった計算が5秒に）
- **通信技術の進歩**
  ADSLから高速光　無線5Gでも2時間の映画のダウンロードが5秒以下
- **リモート会議、遠隔監視、遠隔制御**
  コロナ禍で急激に進展
- **クラウド**
- **AIによる画像処理、音声処理、言語処理**
- **ドローン・ロボット**
- **３Dプリンタ**

写真も複数あると、
関連付けで３次元モデルに

つながることによる「もの」の革新

Industrie 4.0（第4次産業革命：ドイツ） Society 5.0(日本)

⓪ 手動、風力、馬車

① 蒸気機関による大量生産運輸　産業革命

② 電動（コンパクト、強力、コントロール容易）

③ プログラム（マイコン制御、オートメーション）

モノにインテリジェンスがついた

④ インテリジェントが、もの自身からクラウドへ

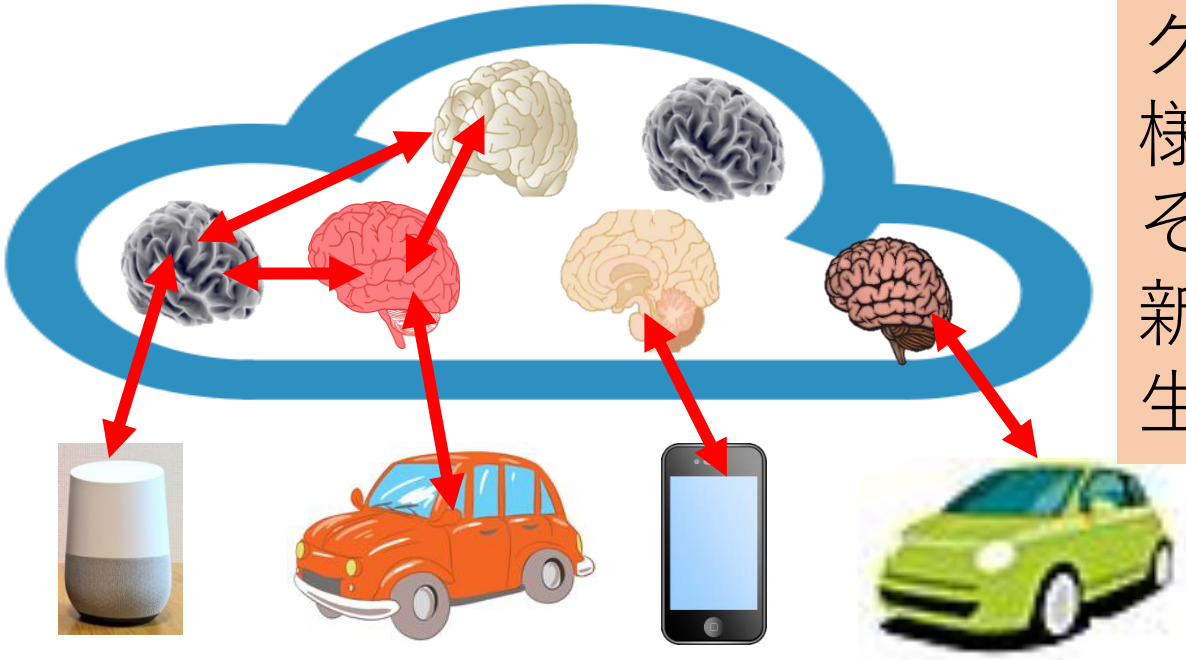
モノからインテリジェンスが離れる

（機能、CPU,メモリ、センサの制限がなくなる）

④って何？

例）iPhoneのSiriは
つながって作動

Cloudでは知能がつながって新たな知能が



クラウドには、
様々な情報が集まり、
それらをつなげると、
新たなサービスが
生まれる

Google Mapの渋滞情報

- Google mapのユーザーは今いる場所の地図を得たいし、経路もナビしてほしいからGPS情報をGoogleに送る
- Googleは膨大に集まるGPS情報から車の移動を推算し、地図上に表示

交通情報のための設備を公共投資→維持管理にも公共投資が必要
ドライバのGPS情報の維持管理→ドライバが自主的に実施　　公共投資は不要

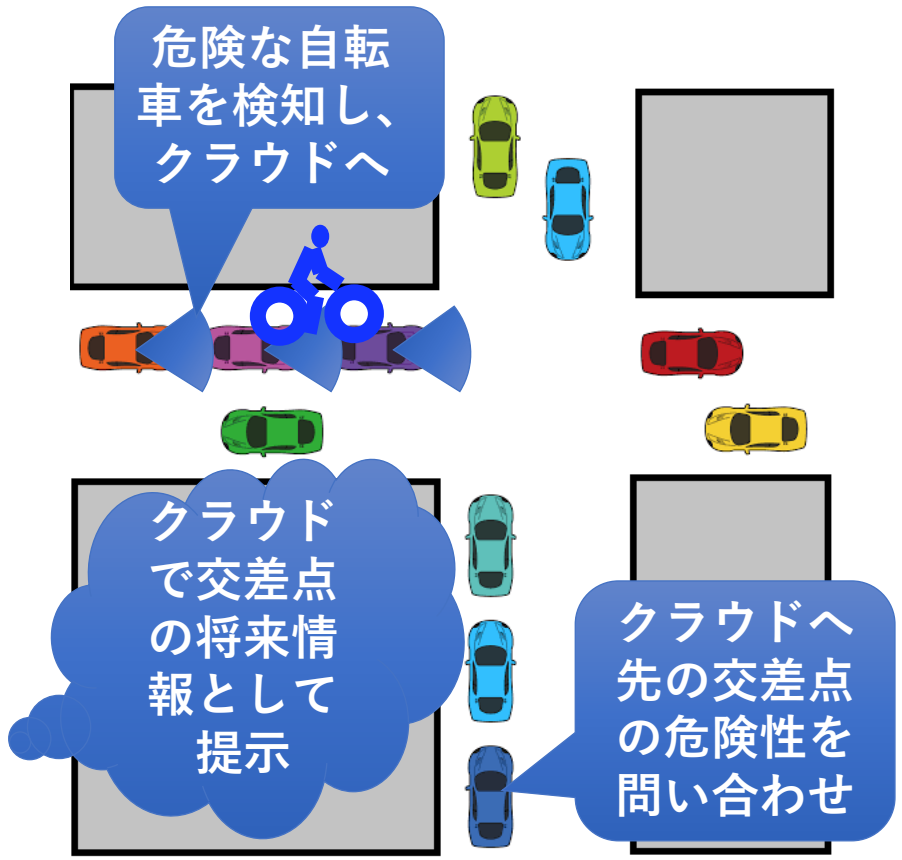
自動運転にはインフラの充実よりもIoT

（課題）ビルの陰からの暴走自転車には？

革新前？

自動車ではなく、自転車がミソ？

→交差点ごとにカメラを設置して、信号機で車に通知？



革新後

→先行車両だけでなく、
別の走行中車両からの情報で、
走行先の交差点の予測を得て、
減速するとともに、
減速することを他の車両に伝え、
危険を回避

→安全向上だけでなく、燃費向上等な効果が期待できる

IoTとクラウドからの情報は、
インフラ投資と無関係にリッチに

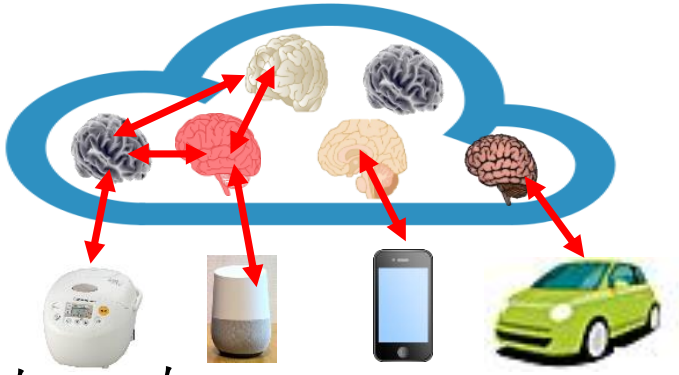
つながることIoTの革新性

インテリジェンスがモノから離れてクラウドへ

- **物理的** (CPU, Memory, HDD, etc.)
- **空間的** (Access to all over the world)
- **時間的** (Past, Present, Predicted Future)

拘束から解放される

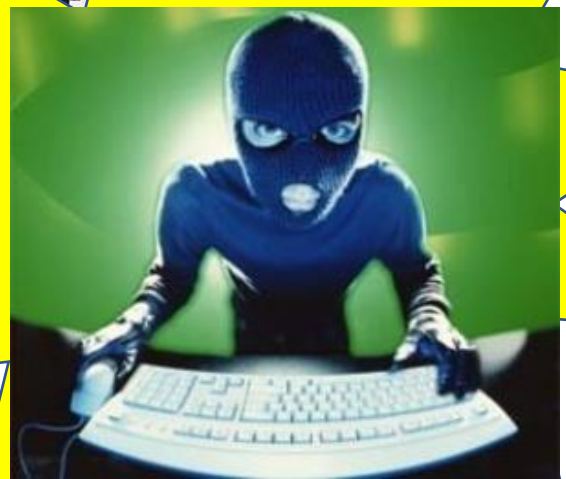
Innovation



System: 特定の**目的**で開発

System of Systems（SOS): 開発時にはなかった**新たな機能**を連動して発揮

AI,自動システム,ロボット,ドローンが暴走したら？



サイバー攻撃で、自由に操作されてしまったら？

物理的被害が発生したサイバー攻撃の例

1. イランの核燃料施設　Stuxnet 2010年
2. ウクライナの変電施設　Black Energy 2015年と2016年
3. ドイツ製鉄所　2014年
4. ダイムラー・クライスラー 操業停止被害17億円 2005年
5. 中東石油化学プラント安全計装　TRITON 2017年
6. ランサムウェア　WannaCry 日立、Honda他多数 2017年
7. Norsk Hydro ラムサムウェア被害にあうも対応の良さで株価上昇2019年
8. 米大規模パイプライン 情報システム被害で操業停止 2021年
9. ロシアウクライナ侵攻でサイバー攻撃激化　2022年
10. 小島プレスのランサムウェア被害で、トヨタ全工場1日停止 2022年

コロナ禍でサイバー攻撃は増えた！

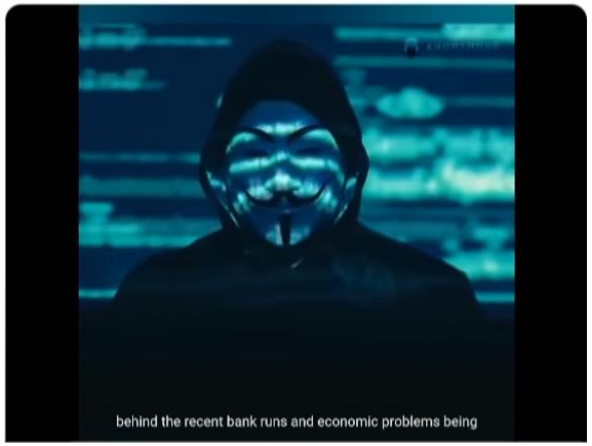
- **フィッシングサイト、フィッシングメール**
  コロナ禍関連で、還付金やネットショッピング関連など様々なフィッシング多発している。
- **マルウェア感染**
  マルウェア（コンピュータウィルス）の発生件数は、３年前の2倍に増加。1年間に1億種類を超える！
  在宅勤務で、家庭内でまず感染して職場へという例も。社内に入れると外部からの進入路を設定できる。
  - **特に**ランサムウェア
    アメリカの大規模パイプラインが運用情報のサーバーを暗号化され、5億円ほどの身代金を支払ったことが有名だが、この例でも身代金よりも長期操業停止という大きな被害が発生している。警察庁の調べでは、2021年上半期は昨年下半期より3倍の61件が発生しその4割弱が1千万円以上の被害を被っている。
    ファイルの暗号化だけでなく、機密情報の暴露やサービスの妨害、取引先への嫌がらせなどを併用し、身代金を要求するなど、凶悪化
    ツール開発、配布、身代金回収が分業化、システム化してきて、ブラックマーケットのビジネスが成立
- **クラウドサービスへの攻撃**
  リモートワークが急増し、社外のクラウドに業務を移動するなど利用が急増したが、その際のクラウドユーザーの設定不備で情報漏洩などの被害が発生している
- **VPN機器への攻撃** **セキュリティ対策自体が攻撃されている**
  社内ネットワークへの接続に利用されるVPN機器に脆弱性があり未対応の機器からIPアドレスやユーザーアカウント、パスワードが大量に盗まれた。複数のメーカーで脆弱性性が発生している。
- **RDP端末への攻撃**
  在宅でのリモートデスクトップ利用が増加したため、その端末に外部からアクセスしてユーザー情報やパスワードを盗む攻撃が増加。入られると、社内にサイバー攻撃が侵攻する。

戦争はサイバーの世界でも

- 2022年2月24日**ロシアがウクライナへの軍事侵攻**を開始
- **ロシアからウクライナへのサイバー攻撃激化**
  - 侵攻前から、サイバー攻撃は激化
  - 1月14日には政府組織にランサムウェア
  - **侵攻直前にワイパーというマルウェアで防衛網の衛星通信を妨害**
  - 侵攻後もDDOS攻撃（サービス妨害）など
  - SPACE-Xがウクライナに衛星通信を提供
  - ウクライナ支援国42か国128組織へもサイバー攻撃
  - **ロシアの情報をウクライナに提供するだけなく、サイバー攻撃には、参戦**
  - **民間人もサイバー攻撃に参加**
- ロシア国内に対する鉄のカーテン
  - ウクライナ侵攻のニュースを伝えるサイトをブロック
- **アノニマスがロシア国営放送をハッキング**
- ベラルーシからの兵器鉄道輸送妨害

物理的攻撃だけでなく、サイバー空間での攻防も

ウクライナを送信元地域とした
跳ね返りパケットの観測数の推移
（引用:JPCERT/CC）



日本でも、工場への被害が多発している

- 2022年3月1日、小島プレス工業がランサムウェアの被害を発表

  トヨタが国内全ての14工場の操業停止を発表

  1社の感染、供給網直撃、関連企業は6万社におよぶ？

  3月2日に操業再開

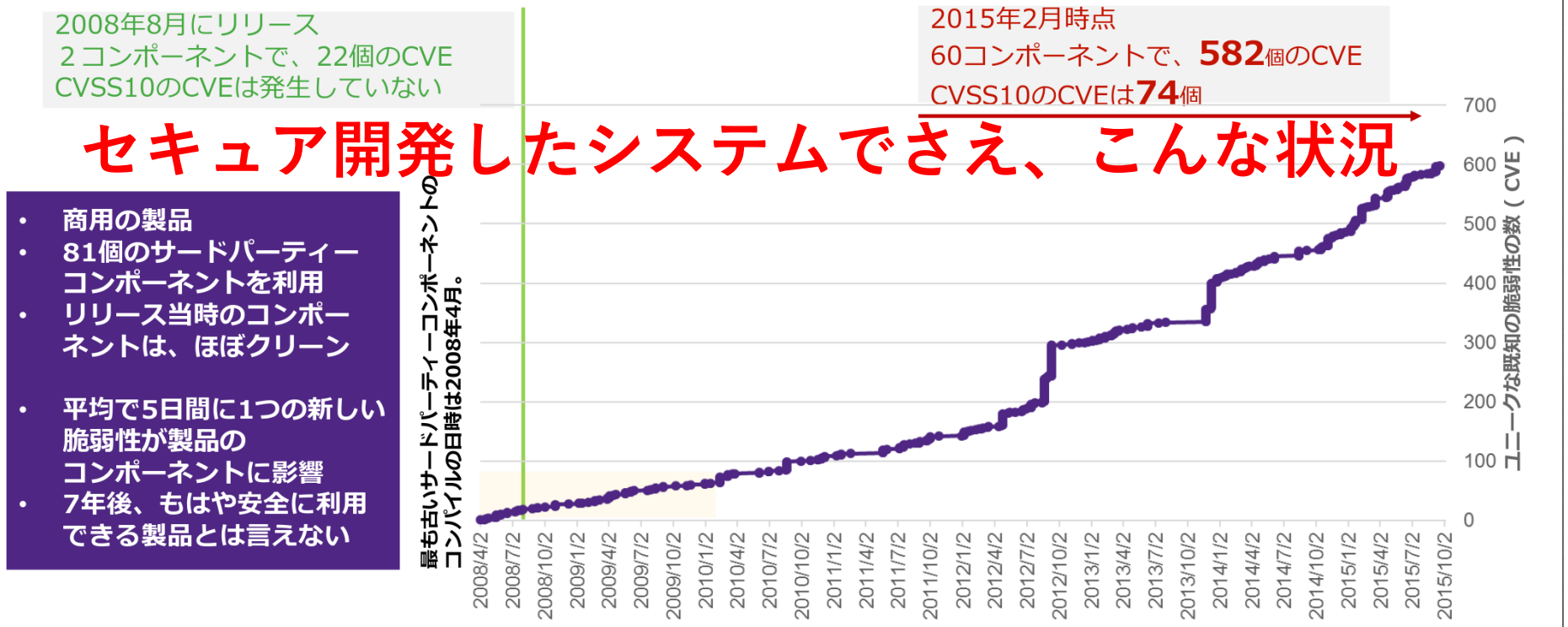
  - 特定企業間の通信に利用するリモート接続機器に脆弱性
  - **小島プレスの子会社**に2月26日に侵入した形跡があった。その後展開
  - ランサムウェアでサーバーなどのデータがアクセス不可になったが、
    要求金額の表示はなく、攻撃者へも連絡していない。
  - サイバーセキュリティ専門家の協力を得て、解析し、
    リモート接続機器からの侵入を特定
  - 情報漏洩の可能性をチェックするとともに、E-mailなどから順次機能復活

情報システムのみの被害でも操業が停止
被害はサプライチェーンに広がる

サイバー攻撃は、続々発明される。

- きりはないし、つねに想定外が発生する。
- 後追いの対策では、疲れるだけだし、
  制御系のセキュリティはイタチごっこについていけない。

時間経過と共にシステムは相対的に脆弱になる



アンチウィルスの検知率は実は驚くほど低い

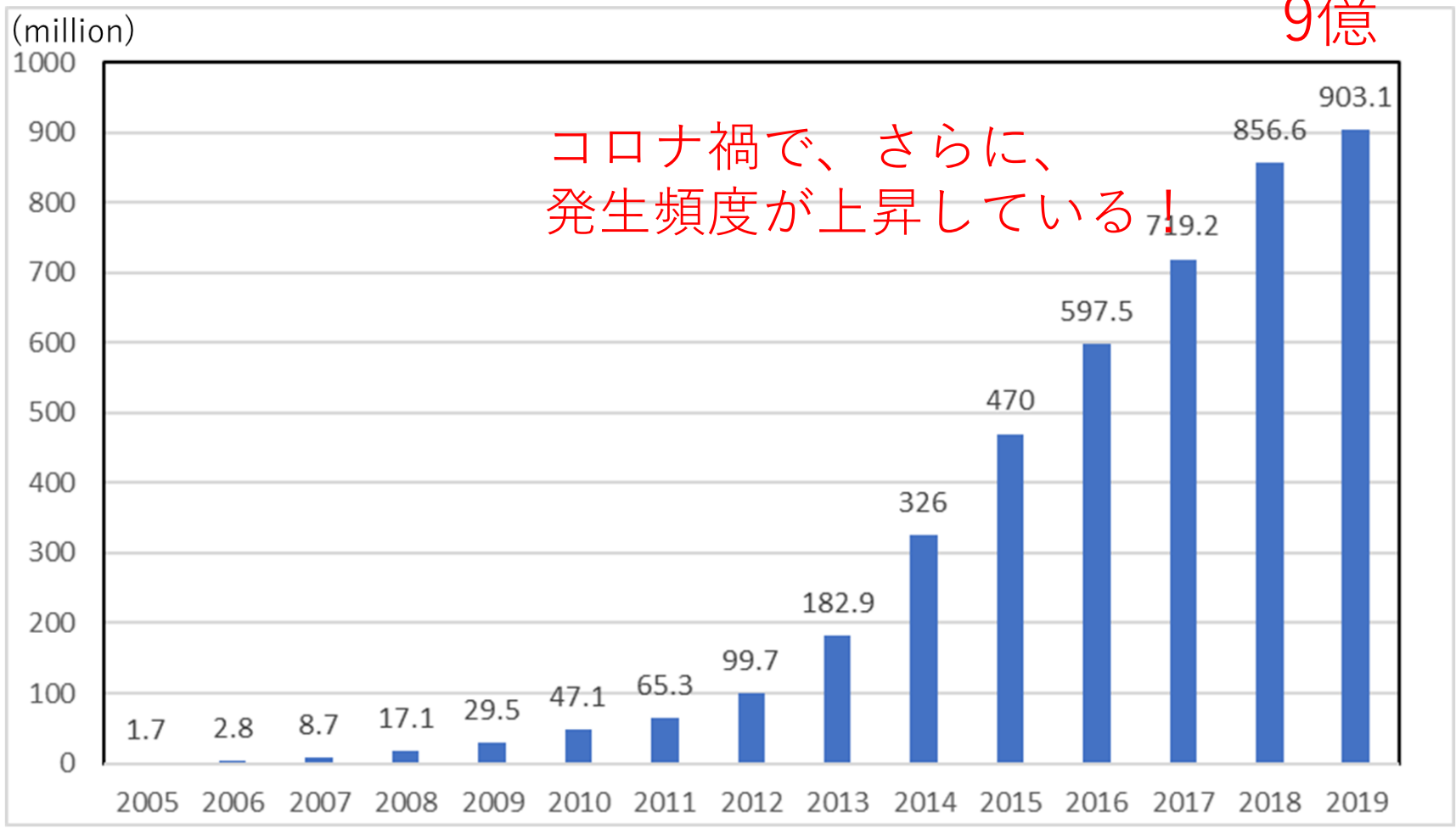


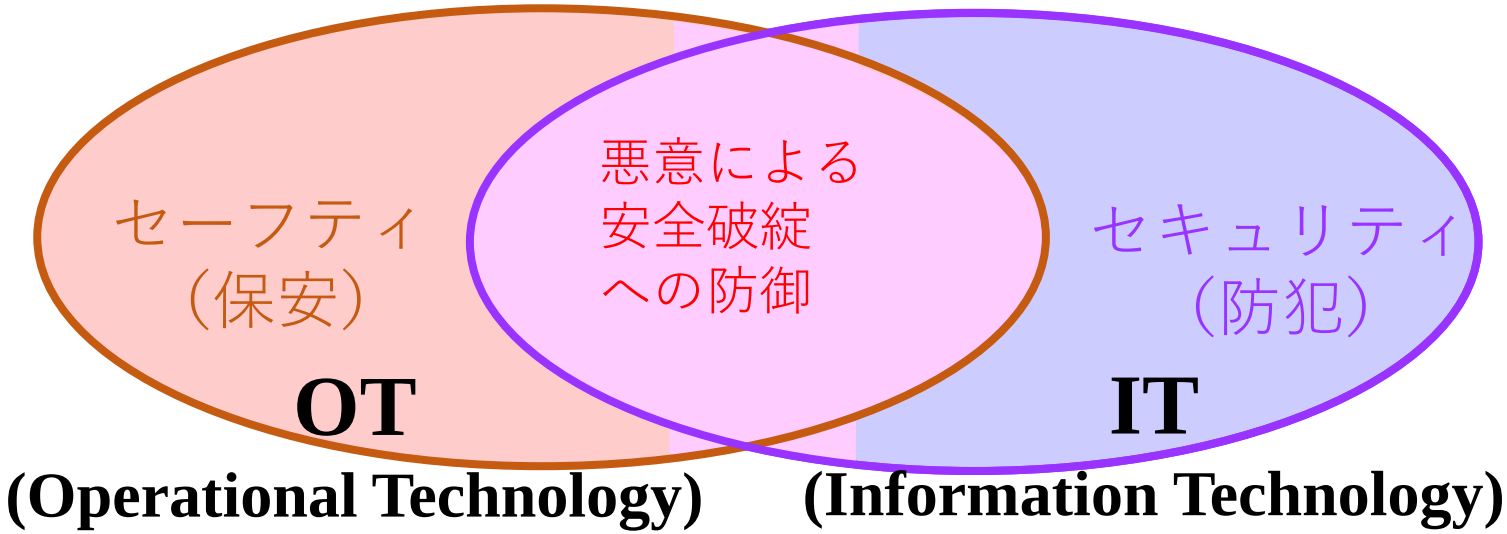
図１．1年間に新たに発生したマルウェアの種類数の推移
2005年から発生したマルウェア種類の積算数

The AV-Test Security Report
https://www.av-test.org/fileadmin/

マルウェア発生
年間1億種類を
超える！

マルウェアは
検知されないことを
確認してから、
リリースされている

SafetyとSecurity



- セーフティの議論では、悪意はほとんど考慮されてこなかった
- サイバーセキュリティは、鍵の頑強化等、防御技術の議論が主であった。
- サイバー攻撃によるセーフティ破綻のリスクまでは検討されていない。
- **安全対策へのサイバー攻撃は、測定端、操作端を含めたコントローラの誤動作**
  - **安全解析で洗い出されたリスク以外の不安全はサイバー攻撃では起こらない**
  - **サイバー攻撃では無効化できない安全対策もある(サーモスタット、リレー等)**

  拠り所の確保
- **セーフティもセキュリティも多重性多層性は共通の防御の基本**
- **ITとOTが協力して、隙間を埋める**

安全を守るサイバーセキュリティには運用が大事

- **ツールがセキュアであっても、その設定や管理で脆弱になる**
  - 設定するパスワードが安直で共通のまま等の設定者の問題
  - フィッシングで内部から攻撃を引き込んでしまう
  - 物理的侵入を許してしまう
  - いくらセキュアに開発しても、脆弱性が発生する
- **脆弱性を放置していたら、安全が破綻する**
  - 脆弱性の発生に気づき対応するのは誰？
- **サイバー攻撃の検知は、どのような段階でどのように検知され、その危険性を評価でき、その対応を誰が実施するのか？**
  - DCS,PLCやSCADAの保守で攻撃が入り込んだ時、誰が何を監視していれば、どんな段階で検知できるのか？
  - 回復には、再発防止が必要だが、その原因解析用のデータは確保できるか？

人・組織が大事

レジリエンスの向上をめざした人材育成

インシデント対応演習（IPA 産業サイバーセキュリティセンター 中核人材育成プログラム）

開発と運用体制の見直し

開発・運用におけるセーフティとセキュリティ確保

■ 課題１：安全設計の後でセキュリティを考慮することでの手戻りの防止

従来から安全は意識されてきているが、セキュリティは盗難防止ぐらいかも。

例えば、セキュリティ強化で通信を暗号化すると遅れが発生する。
そのために、ブレーキシステムなどの再設計が必要になるかもしれない。

セキュリティをセーフティと同時に検討するには？

■ 課題２：開発後にも発生する脆弱性のライフサイクルに渡る管理

セキュア開発として、脆弱性が発生しない開発は意識されてきた。

開発中の脆弱性発生の防止も容易ではないが、
常に新たな脆弱性が発生し、開発後に発生した脆弱性に対応しないと、
安全が破綻する可能性がある

だれが、どのように脆弱性の発生を検知し、対応を管理するのか？

提案手法

解決策 (1)　セーフティとセキュリティを同時に考慮できるモデル表現

情報の流れを表現するDFD(Data Flow Diagram)による機能表現

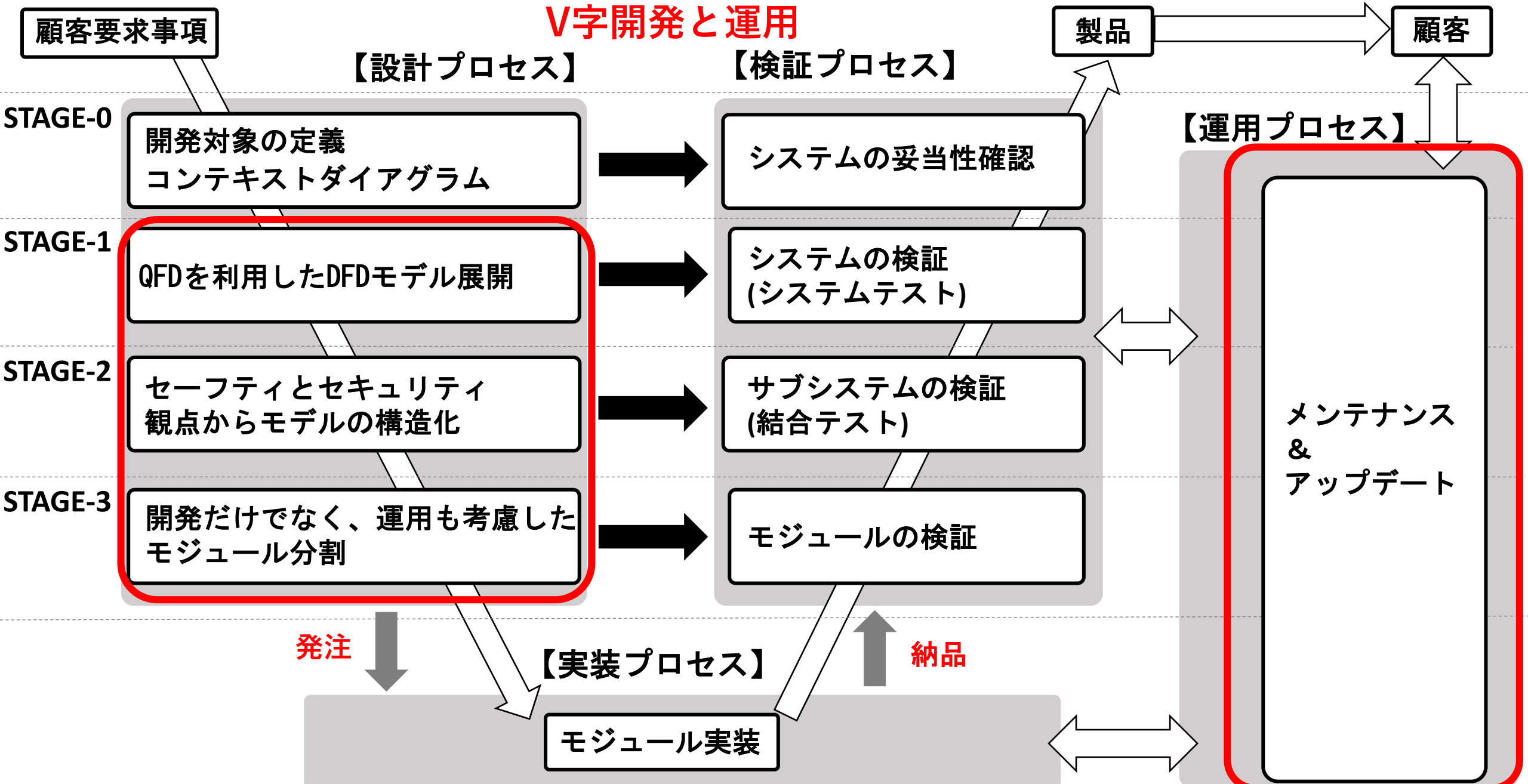
解決策 (2)　セーフティを確保する機能を、モジュールの組合せで表現し、
そのモジュールおよびモジュール間通信のセキュリティを検討

そのモジュールの異常の検知と異常時の代替案を検討

解決策 (3)　SBOMの徹底と将来に渡る脆弱性管理の責任の明確化

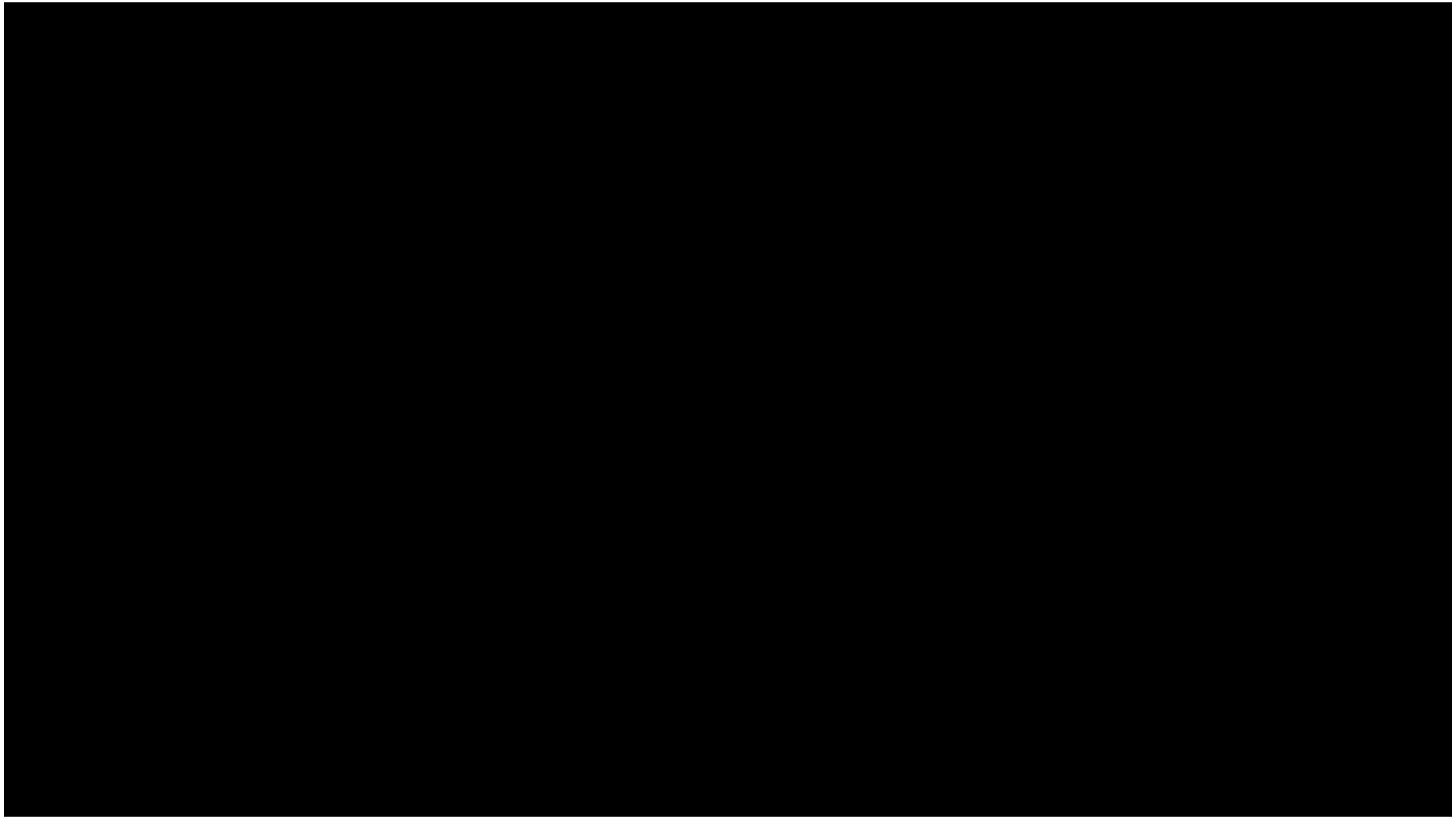
モジュールの開発を委託する際に、
開発時だけでなく、将来に渡って脆弱性に責任をもって取り組むか
開発後、委託元が脆弱性管理が可能な情報をすべて提供する契約にする

セーフティとセキュリティを確保するシステムのライフサイクル



セーフティとセキュリティを考慮したシステム開発

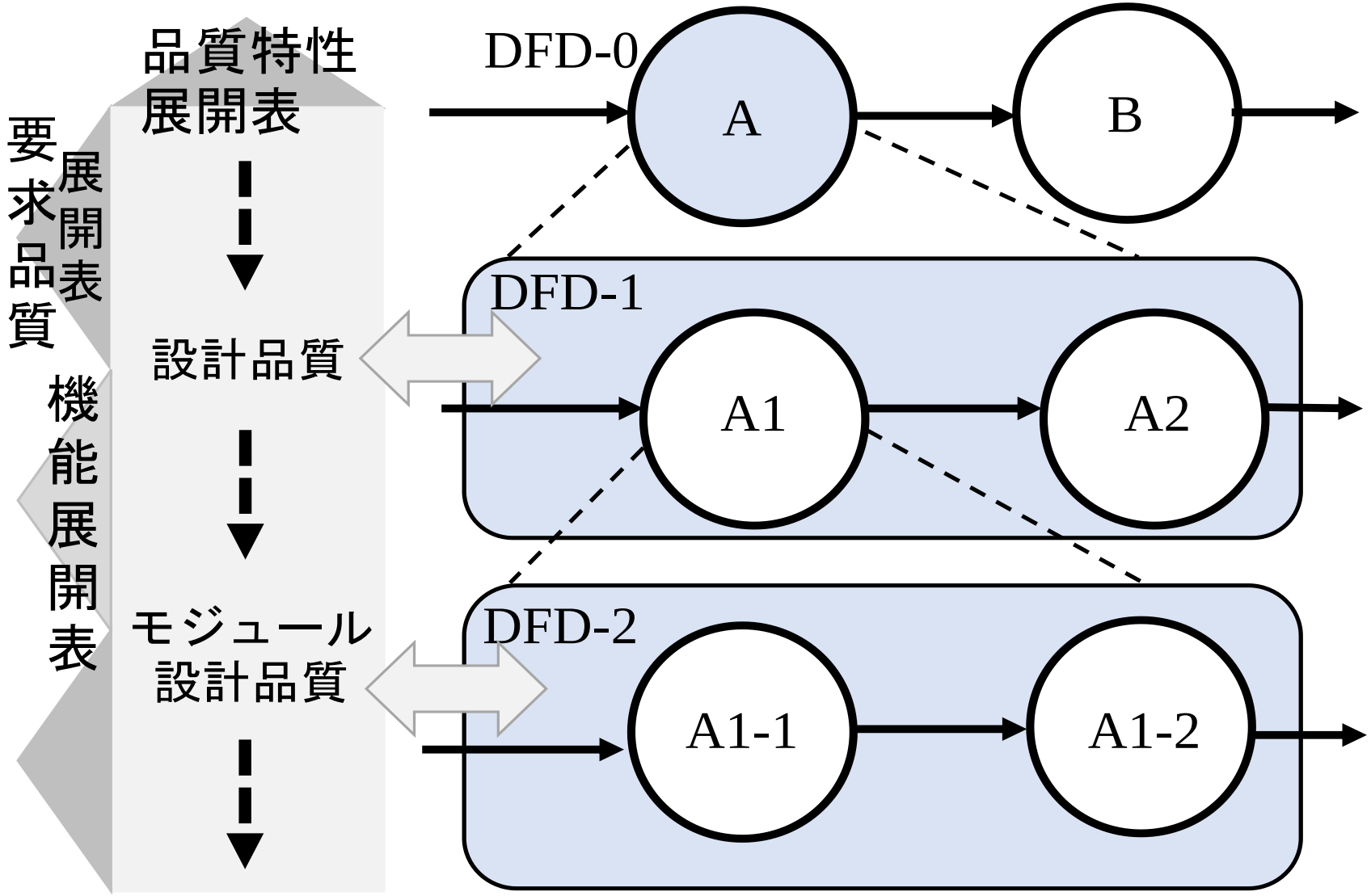
研究室で開発した自動運転車いすを題材にシステム開発を検討する



https://web.manage.nitech.ac.jp/Security/autodrive_wheelchair.mp4

Stage-1:　QFDを利用したDFDモデル展開

QFD(Quality Function Deployment)　　DFD(Data Flow Diagram)

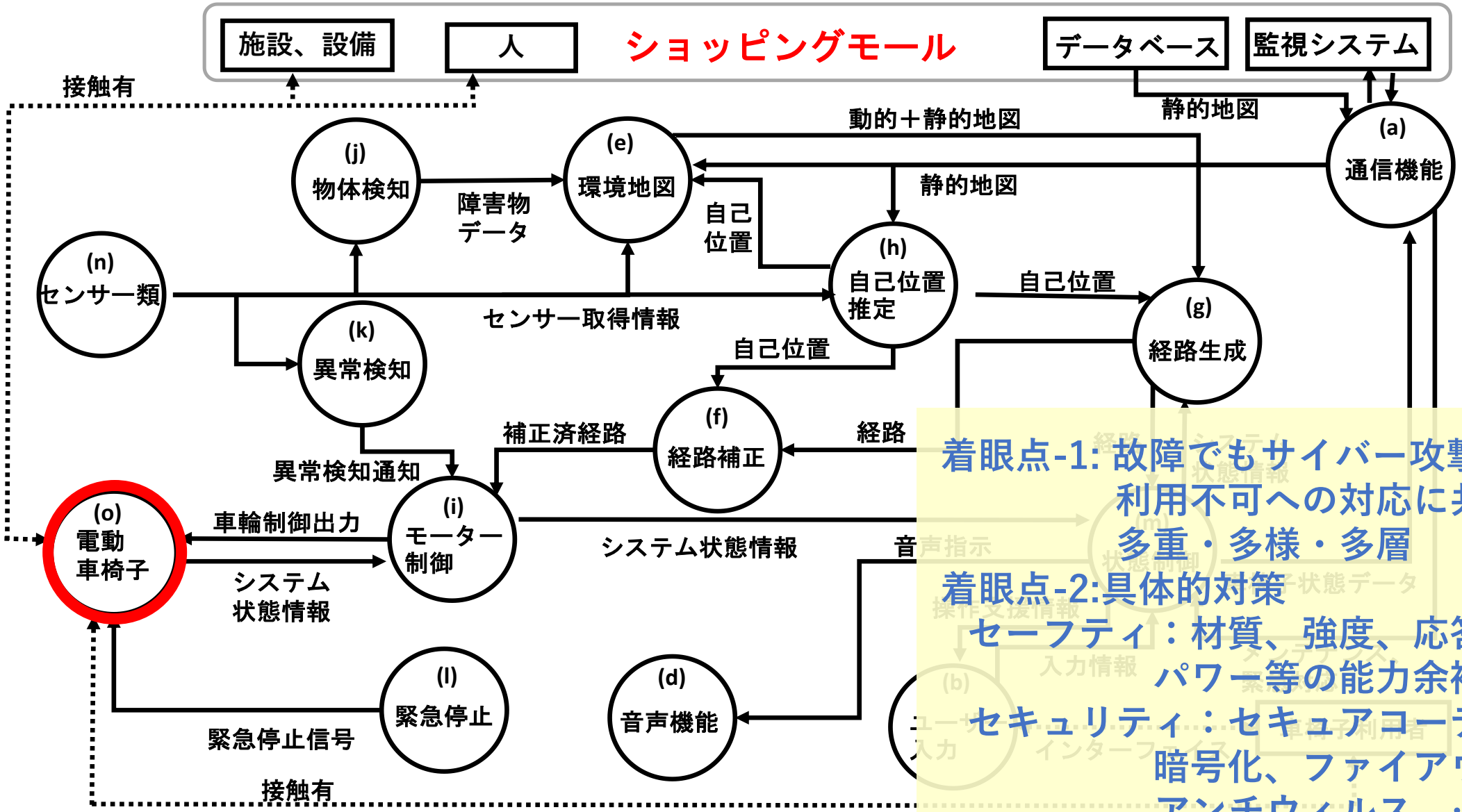


セーフティの面も
セキュリティの面も
共通に議論できる
QFDとDFD
で表現する

機能は健全でも
入力データが
間違っていれば
不適切な挙動につながる

不健全な機能の影響除去と
代替案の確保

Stage-1: Dataの流れに注目して機能表現で セーフティ機能とセキュリティ機能を検討



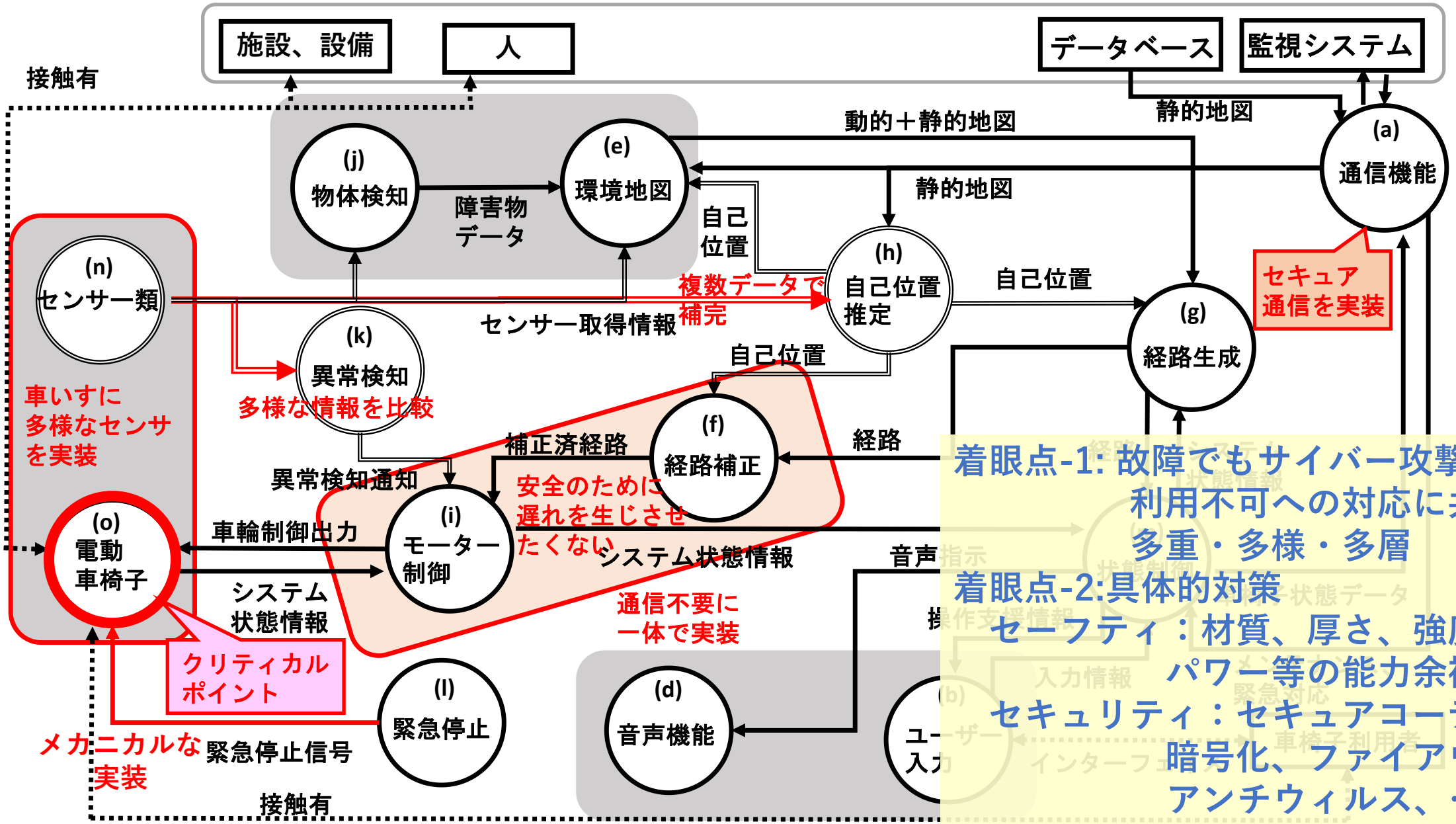
着眼点-1: 故障でもサイバー攻撃でも
利用不可への対応に共通性
多重・多様・多層

着眼点-2:具体的対策

セーフティ：材質、強度、応答速度、
パワー等の能力余裕、…

セキュリティ：セキュアコーディング、
暗号化、ファイアウォール、
アンチウィルス、…

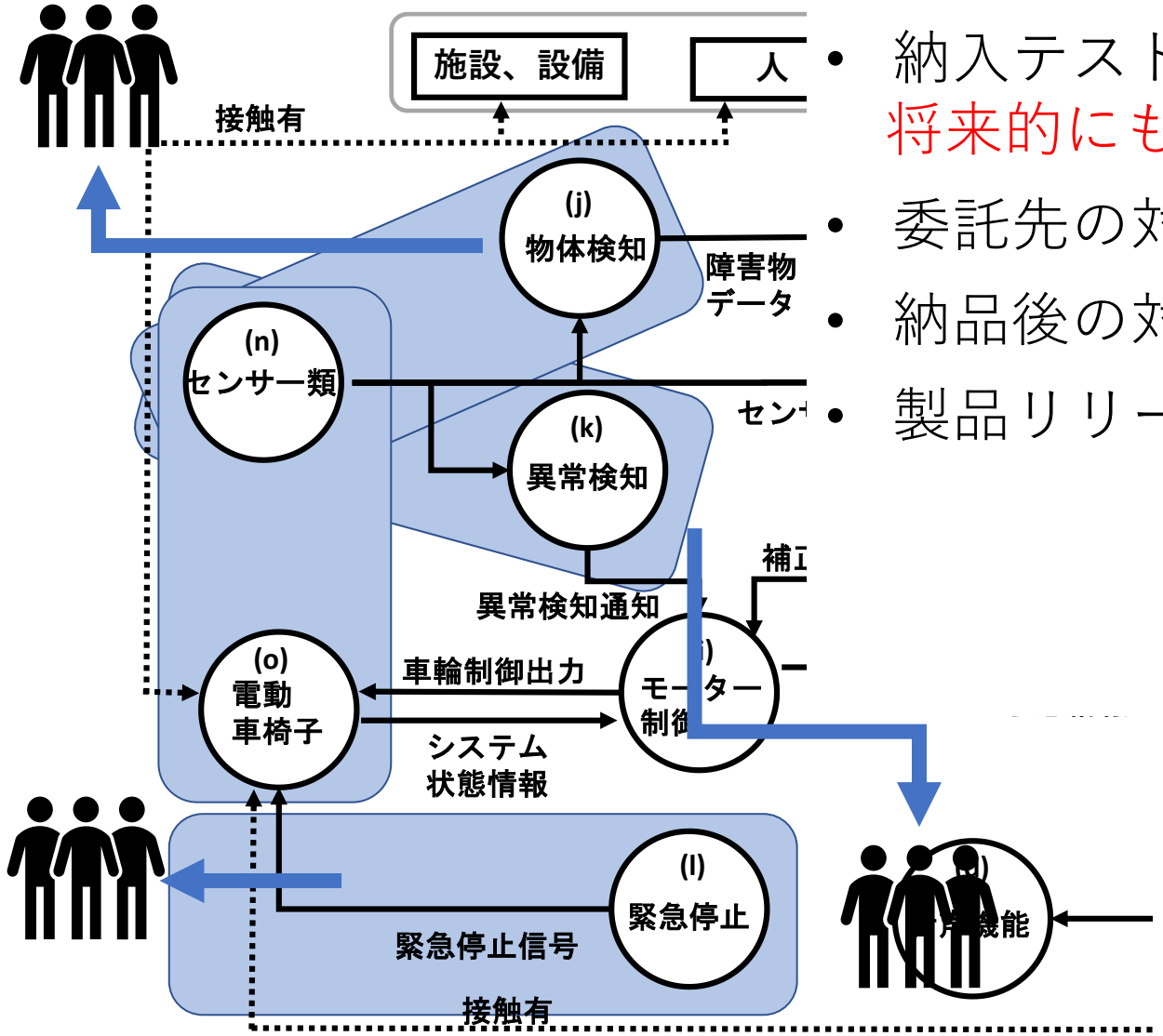
Stage-2: セーフティとセキュリティ観点からモデルの構造化



着眼点-1: 故障でもサイバー攻撃でも
利用不可への対応に共通性
多重・多様・多層

着眼点-2:具体的対策
セーフティ：材質、厚さ、強度、
パワー等の能力余裕、…
セキュリティ：セキュアコーディング、
暗号化、ファイアウォール、
アンチウィルス、…

Stage-3: 開発だけでなく、運用も考慮したモジュール分割



Stage3では、モジュール開発の**外部委託**に注目

- 納入テスト時に、仕様通り稼働することだけではなく、
  将来的にも、そのモジュールの健全性を保証する必要
- 委託先の対応能力の確認
- 納品後の対応を可能ための納品物の条件
- 製品リリース後の管理体制

開発時の選択

- 一部の安全に重要なモジュールは
  外部委託せず、社内開発
- 破綻することを前提に、
  多重多様にモジュールを確保することで
  外部業者の対応能力に依存しない

SBOM（Software Bill of Materials)による脆弱性管理

利用しているモジュールのリストを脆弱性データベースで参照

Component	Version	CVE	CVSS	Object full path
openssl	1.0.2h	CVE-2020-1968	4.3	OPCsvr1_Plant2-disk1.vmdk:Windows/Installer/dfd6c.
glib		CVE-2020-6750	4.3	OPCsvr1_Plant2-disk1.vmdk:Windows/Installer/dfd6c.
7zip	9.2	CVE-2018-5996	6.8	OPCsvr1_Plant2-disk1.vmdk:Windows/Installer/dfd6c.
gettext		CVE-2018-18751	7.5	OPCsvr1_Plant2-disk1.vmdk:Windows/Installer/dfd6c.
libjpeg		CVE-2020-14151	5.8	OPCsvr1_Plant2-disk1.vmdk:Windows/SysWOW64/qu
libtiff		CVE-2019-7663	4.3	OPCsvr1_Plant2-disk1.vmdk:Windows/SysWOW64/Wi
mesa		CVE-2019-5068	3.6	OPCsvr1_Plant2-disk1.vmdk:Windows/SysWOW64/vm
libpcap	1	CVE-2		
libpng		CVE-2		
coreclr		CVE-2		
sqlite3		CVE-2		
pcre		CVE-2		

脆弱性データベースと連携して脆弱性発生を把握

CVE(Common Vulnerabilities and Exposures)

NVD(National Vulnerability Database)

JVN(Japan Vulnerability Notes)

2021年5月アメリカ大統領令

SBOM（Software Bill of Materials)

どこにどんなモジュールが利用されているか管理する。

脆弱性データベースと連携して脆弱性発生を把握

CVE(Common Vulnerabilities and Exposures)

NVD(National Vulnerability Database)

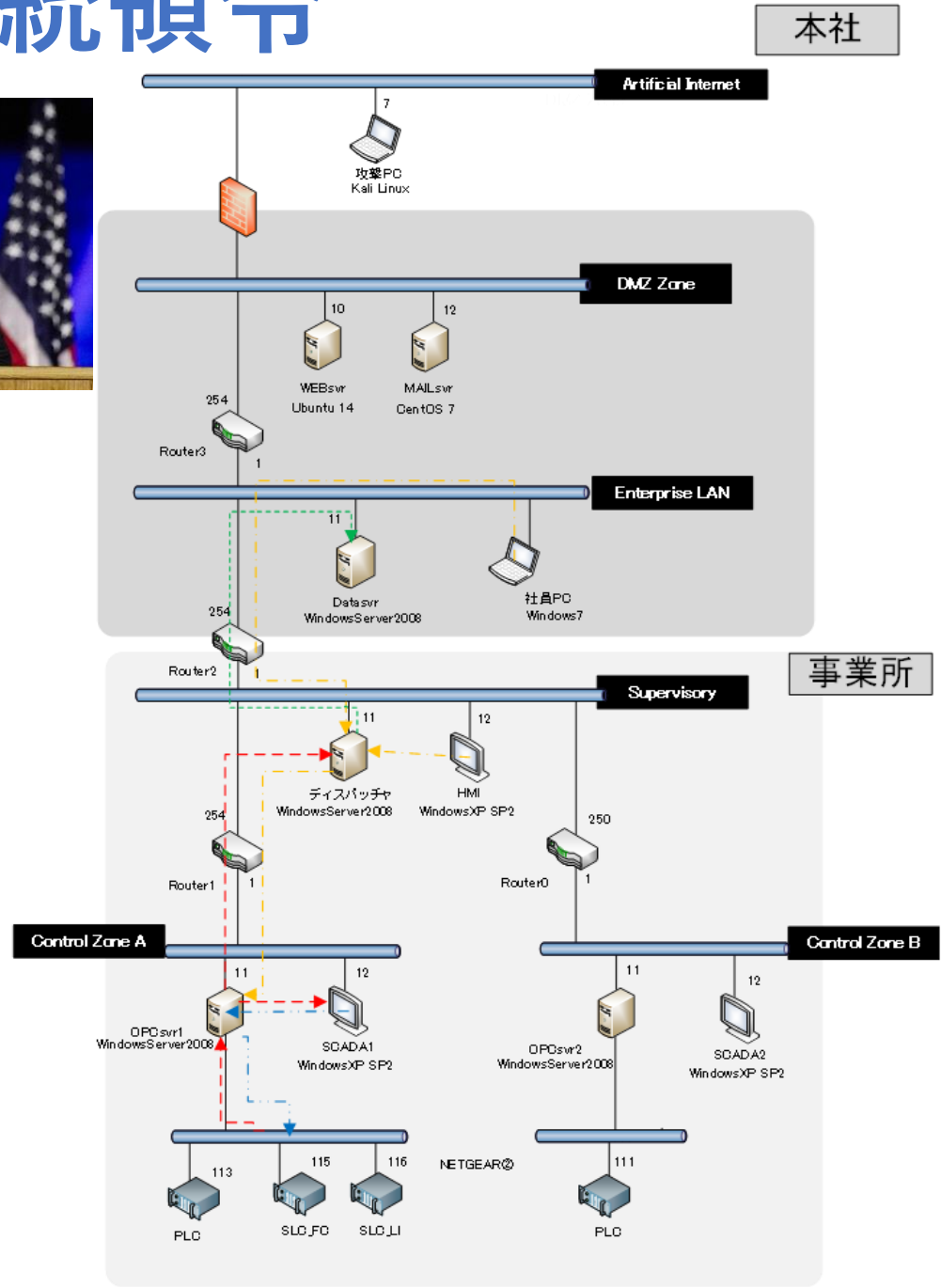
ライフサイクルに渡った脆弱性管理を実現

ゼロトラスト（水際では防ぎきれない！）

多層防御で、ここは信頼できるゾーンという範囲を
確保しようとするのが、基本ではあるが、

すべての通信に多要素認証や通信監視の導入

安全性を考えると、物理的侵入も含め、
攻撃は多彩・巧妙になっており、
ここは信頼できるという前提を置くことは危険である
水際の監視よりも、被害発生個所に近い箇所の監視を重視し、
すばやく対策をとることが必要になる。



まとめ

つながることの価値を活かす
Safety and Security by Designのアプローチ

- **つながることには、革新性が期待される。**
- 自動運転に限らず、様々なものに安全＆セキュリティの問題
- **脆弱性は発生しつづけるので、運用を重視した開発が大事**
- 故障でもサイバー攻撃でも、多重多様多層な対策で、
  一部に破綻が生じても安全は確保できるように考える。
- **モジュール開発の委託には、仕様通り動くことだけでなく、
  将来的な脆弱性発生への対応も期待したい。**
- SBOMの普及と脆弱性対応体制の確保が望まれる。

自己紹介　橋本芳宏

名古屋工業大学 社会工学科 経営システム分野　教授

https://web.manage.nitech.ac.jp/Security

（制御系セキュリティに関して）

2011年～2012年　経済産業省
　制御システムセキュリティ検討タスクフォース材育成WG委員
2012年～2014年　IPA（情報処理推進機構）
　制御システムワーキンググループ委員
2016年～　内閣府 戦略的イノベーション創造プログラム
　重要インフラ等におけるサイバーセキュリティの確保
　セキュリティ人材育成 委員
2017年～　IPA産業サイバーセキュリティセンター講師

名古屋工業大学制御システムセキュリティWS開催

　2015年3月19, 20日 から 2018年9月3, 4日　半年に1回
　　計装ベンダー, ユーザー, セキュリティベンダー, 官庁等
　　から参加者を得て開催
　研究室でのサイバー攻撃のデモには2013年からのべ500名以上

（プロセス制御に関して）

2010年～　計測自動制御学会 プロセス塾講師

（略歴）

1985年　京都大学化学工学専攻博士課程（単位取得退学）
　「蒸留塔における組成制御のための操作変数の選定」に関する研究
1985年　名古屋工業大学 生産システム工学科 助手
2003年　名古屋工業大学 システムマネジメント学科 教授
　学内組織再編を経て、現在にいたる
2023年3月 定年退官予定