組織内ネットワークのセキュリティ被害軽減対策におけるSTAMPモデリングの試行

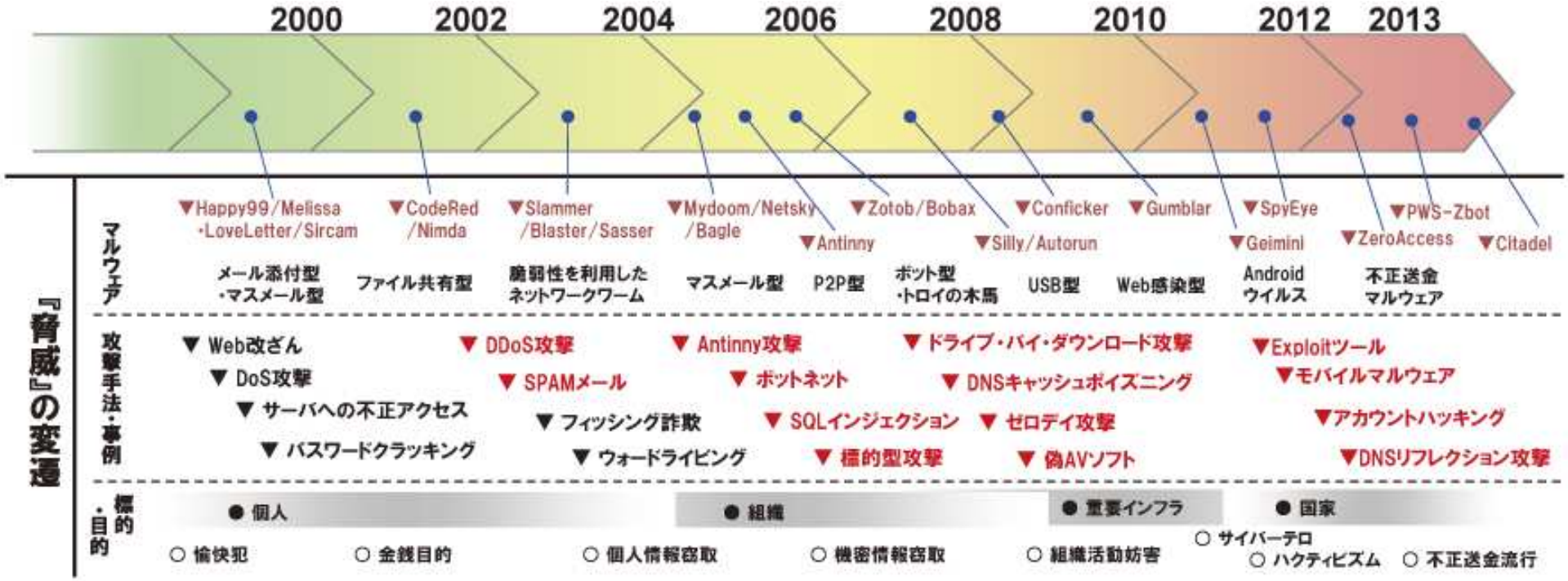
2016/12/6

長崎県立大学 情報システム学部
加藤 雅彦、日下部茂

背景

脅威の変遷 The changes of The Internet threats

- ネットの脅威は変化し続けている

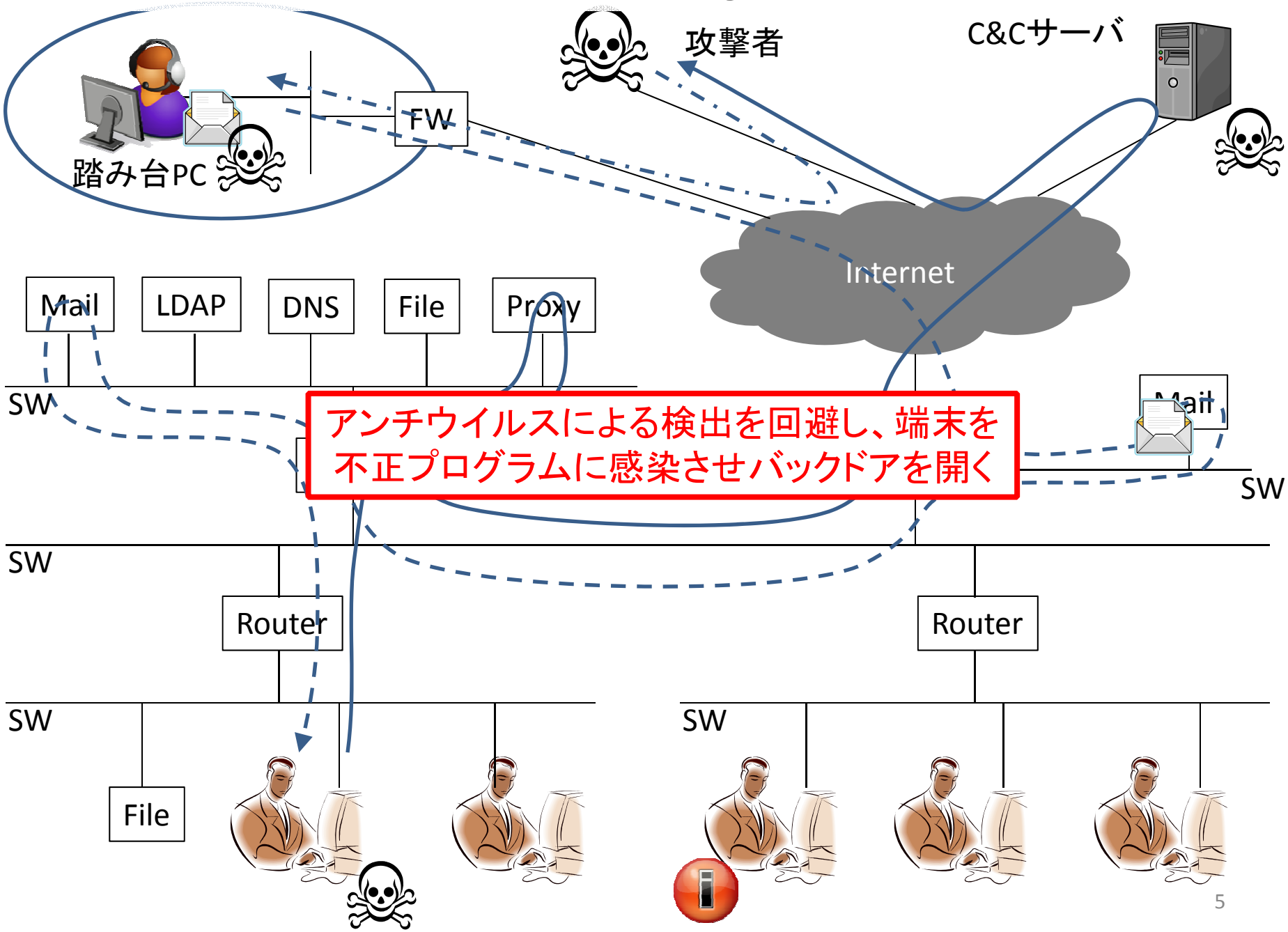


総務省H26白書から引用

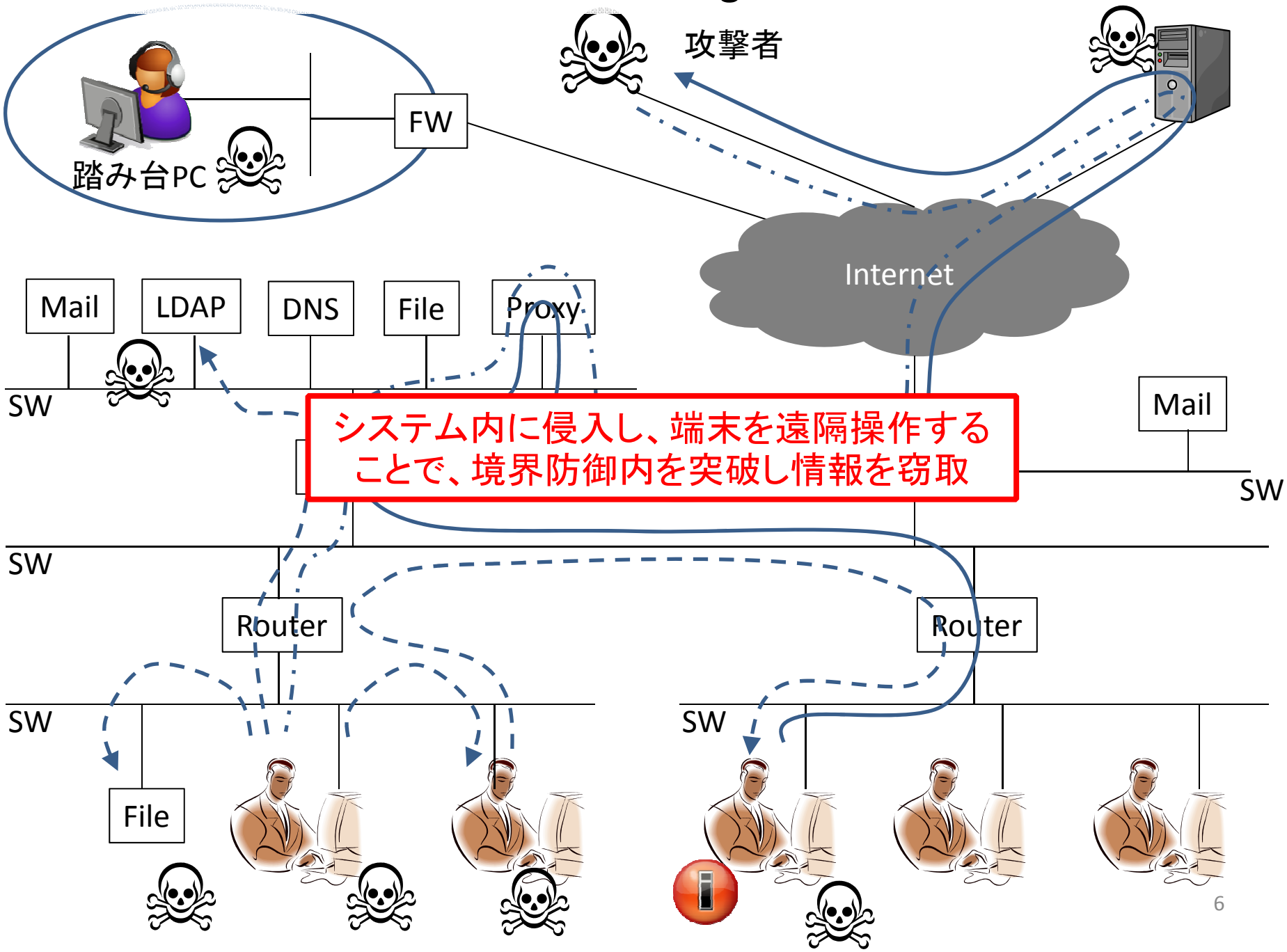
標的型攻撃 Targeted attack

- ある特定の組織や人物を標的として、
- ソーシャルな手段を利用しつつ複数の段階を経て、
- 様々な攻撃手法を組み合わせ、
- 持続的に組織内ネットワークに侵入し、
- 最終的に情報の窃取やシステム破壊などを行う攻撃

近年顕著な標的型攻撃　A flow of targeted attacks



近年顕著な標的型攻撃　A flow of targeted attacks



攻撃の高度化

IPAセキュリティセンター発行の関連ガイド

- 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」(2011年8月,11月)
- 「『標的型メール攻撃』対策に向けたシステム設計ガイド」(2013年8月)
- 「『高度標的型攻撃』対策に向けたシステム設計ガイド」(2014年9月)
  - 従来対策：初期潜入段階
  - 内部対策：基盤構築、内部侵入・調査段階

事例：日本年金機構
Example: The data breach of Japan Pension Service

- 標的型攻撃による情報漏えい
- 被害拡大防止のためインターネット接続を遮断
- 想定外の攻撃のため、極端な対応をせざるを得なかった

（2）標的型攻撃を想定したシステム設計及び運用の不十分性

機構においては、基幹系システムの刷新計画が優先され、機構 LAN システムに内在し標的型攻撃を引き起こす可能性のある種々の脆弱性には注意が払われ

（1）機構 LAN システムと基幹系システムの分離の不徹底

上記２で示した通り、機構のネットワークシステムは、大きく社会保険オンラインシステムと機構 LAN システム等の情報系システムの二つのシステムから構成されている。このうち、年金に関する個人情報は基幹系システムにおいて処理を行うこととなっており、機構 LAN システムではこうした個人情報に関する処理を行うことはないというのがシステム構成の前提となっていた。すなわち、取り扱う情報の種類によって利用するシステムの分離が図られていた。

しかしながら、機構においては、業務の必要を理由に、事務処理を行う機構 LAN システムへの個人情報の移管・保管が一定のルールの下で認められ、機構 LAN システム上の共有フォルダに個人情報が置かれるという、上記のシステム構成の前提に反する運用が行われていた。共有フォルダへの個人情報の保存に際しては、アクセス権の設定、または、パスワードの付与というルールが規定されていたが、インターネットからの標的型攻撃を想定した場合、こうした運用は適切なものとはいえない。

日本年金機構における不正アクセスによる情報流出事案検証委員会「検証報告書」P9~P10より引用

サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」より引用

被害を軽減するために、本来はどうすべきか?
What we should do for mitigating damage?

業務を継続しつつ、情報の漏えいを止める
Stopping information leakage and continue business

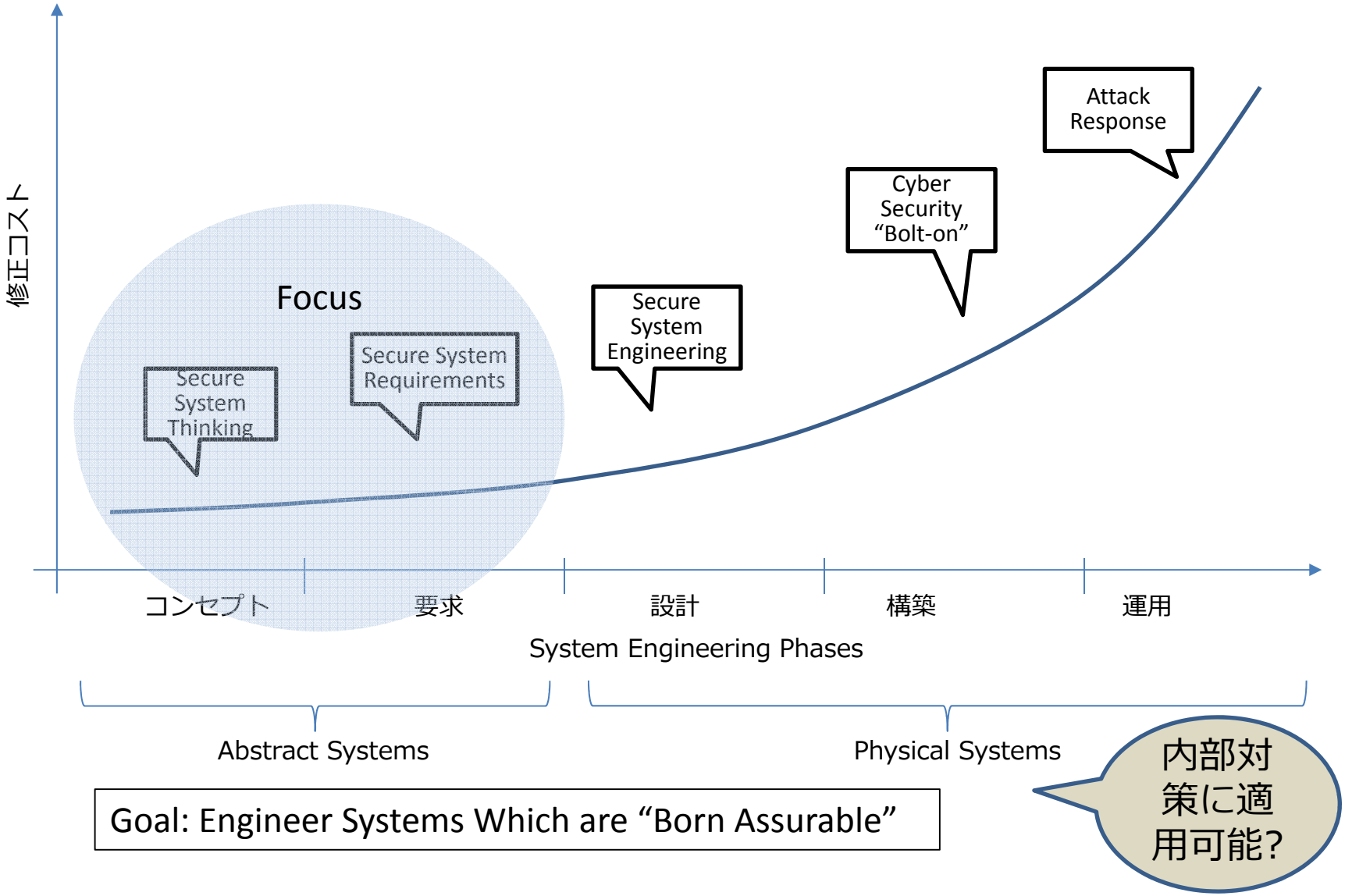
- 攻撃を検知する仕組みの導入
  - 「攻撃」となる通信の定義
    - 業務に必要となる通信以外は「攻撃」とする　　・・・など
  - 「攻撃」を適切に検知、遮断するための技術要素の導入
    - 検出機器から、運用者や連係して動作する機器へ、適切なタイミング、適切な方法で、適切な情報の提供が必要
  - 上記技術要素の適切なシステムへの組み込み
    - 情報が検出装置を通らなければ検出できない
  - これらを運用する体制
    - 機器からの出力を適切に判断して、組織でマネジメントできなくてはならない

業務を継続しつつ、情報の漏えいを止める
Stopping information leakage and continue business

- 攻撃検知後の対応
  - 「攻撃」を検知した後の適切なアクションの定義
    - いつ、だれが、何を、どのようにするのか
      - セキュリティ技術者による攻撃内容分析
      - 運用担当などによる、業務への影響分析
    - いつ、だれに、何を報告するのか
      - 運用担当からの適切な組織内エスカレーション
      - 責任者による、暫定対策の判断
      - 責任者による対策実施指示

STAMP/STPA(-Sec)を試行
Try to apply STAMP/STPA(-Sec)

STPA-Sec Motivation



Goal: Engineer Systems Which are "Born Assurable"

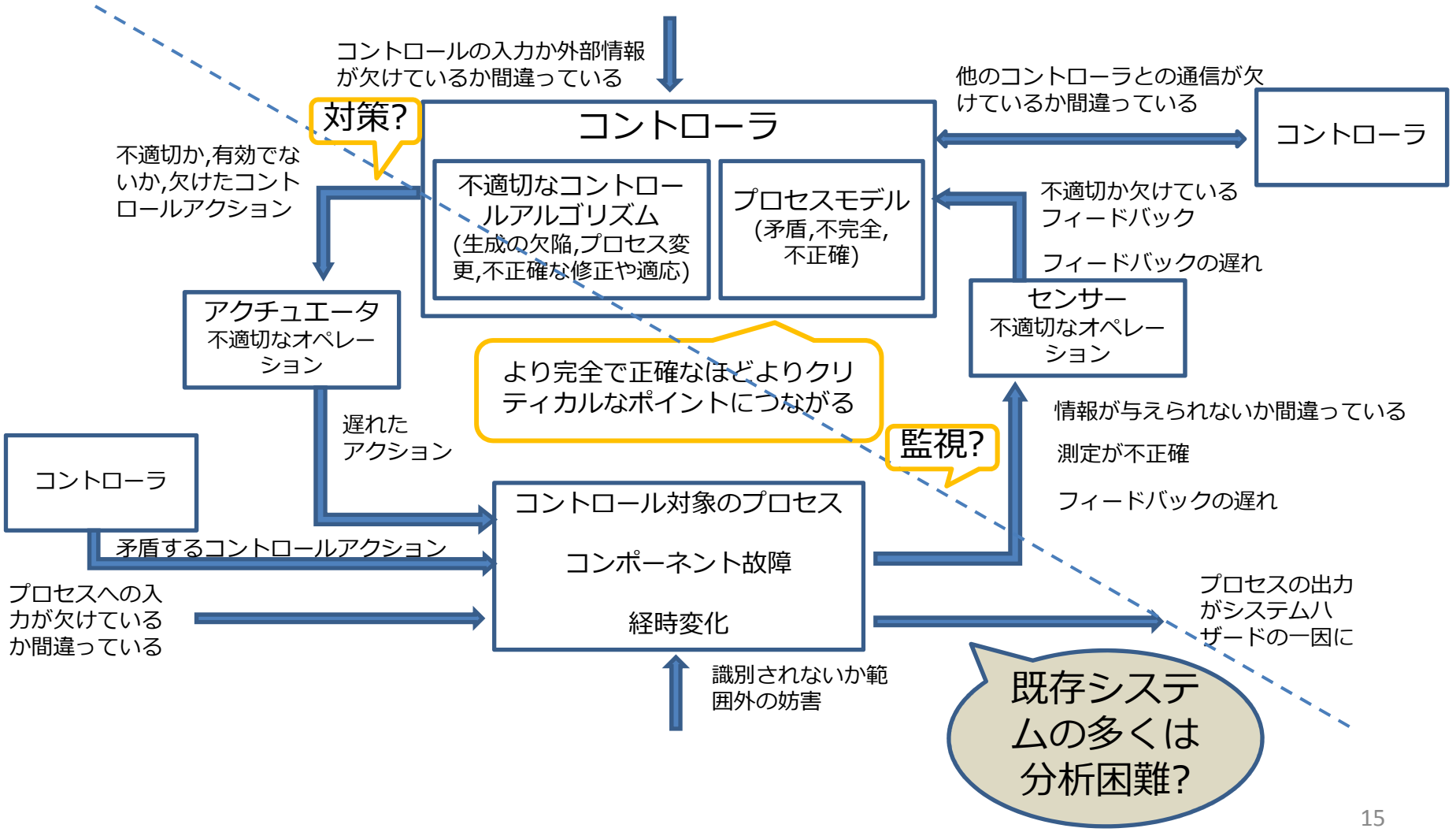
モデル基本要素の準備
Preparation of the model basic elements

まずアクシデント，ハザード，安全制約を決定

- アクシデント
  1. 知財情報などの窃取・偵察(IPAガイドより)
  2. ITシステムの破壊・妨害(IPAガイドより)
  3. 業務が継続できない(追加)
- ハザード
  1. 攻撃者の攻撃基盤を構築を防止できない
  2. 侵害の拡大を防止できない
  3. 業務継続に必要な要件が判断できない
- 安全制約
  1. 攻撃者の攻撃基盤を構築を防止できない
  2. 侵害の拡大を防止できる
  3. 業務継続に必要な要件が判断できる

コントロールストラクチャ構築
Building control structure

- 対策担当者はどのような分析を?



(STAMP/STPAも用いた)厳密な分析に向けて
What is necessary for strict analysis

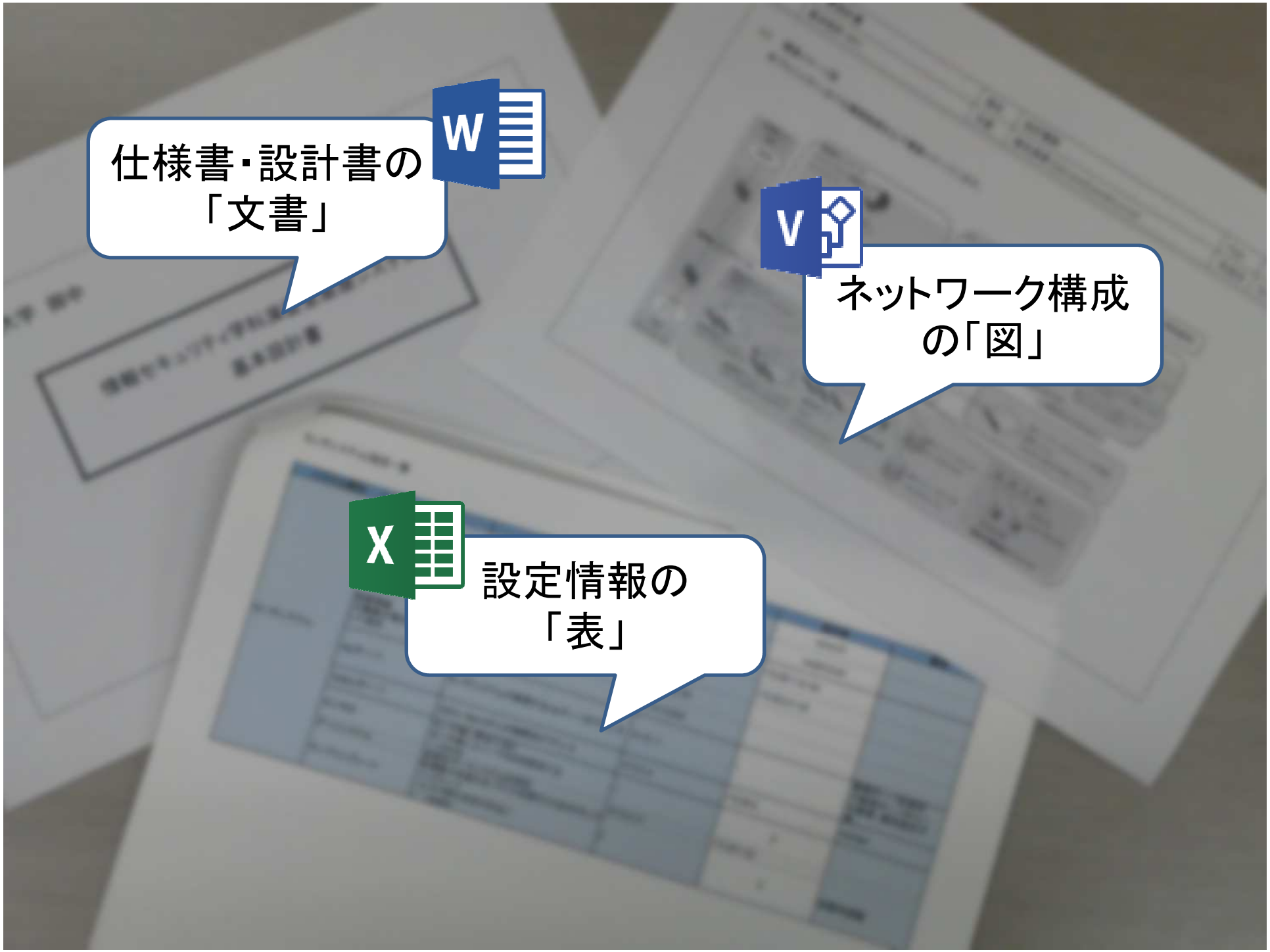
阻害要因：人に依存した不正確な情報とその管理
Negative factor: Information security management by personal effects

- 物理的接続や部分的な通信要件など記載された断片情報
- 業務とシステムの関係を考慮しないインフラストラクチャ
- 人が読むために作られた（再利用性の低い）ドキュメント
- 業務優先で、設計情報と実態が異なるシステム運用

管理不能なシステムへ

阻害要因：属人的システム設計構築情報
Negative factor: Information security management by personal effects

- 初期のシステム構築で最低限必要な機能要件を実装
  - 非機能要件の実装が漏れる
- 実装後、機能拡張などで共通インフラ上に数多くの業務を共存
  - システムの相互依存関係などが不明確となる
- 設計の考慮漏れを実装時に解決するため、設計情報と実装のミスマッチが発生
  - 作業者、過去のドキュメント、実装にズレ
- 担当者の異動、退職等により設計意図や運用ノウハウが消滅


仕様書・設計書の
「文書」
ネットワーク構成
の「図」
設定情報の
「表」

ポイントは何か?
Necessity for grasping an information flow

- 業務に必要な「情報の流れ」を把握する
  - どの組織がどのような業務を行っているかを特定
    - 重要な情報を扱う業務はどの程度安全な通信を行う必要があるか
    - 緊急対応として行われる業務はどの程度優先的に処理されるべきか　　・・・など
  - どの業務がどのようなシステムに依存しているかを特定
    - 業務Aが使うシステムと業務Bが使うシステムは疎結合か密結合か（Bが出来なければAが動かない）
    - どこまで共通のインフラを使用しているか（通信回線や名前解決は共通のインフラを使いがち）　　・・・など
  - どのシステムがどのような通信を行っているかを特定
    - インターネットがないと使えないシステム
    - インターネットがなくても使えるシステム　　・・・など

機械処理可能なシステムモデルの活用
Utilization of machine processable system model

- システムの仕様を反映した、機械処理可能な形式モデルを使えば、複雑なシステムでもセキュリティ対策による業務影響を分析でき、妥当な対策を実施できる?

どうやって有用な形式モデルを構築する?
→　STAMP/STPA(-Sec) ＋ 形式仕様記述

今後の課題 Future work

- コストや納期、担当者のスキルに限界があり、厳密なシステム要件定義、実装を行うことは困難な場合が多い

- STAMP/STPA(-Sec)によるセキュリティ対応の設計精度向上がどこまで可能か
- 形式的な記述による厳密なシステム定義はどこまで可能か
- IoTシステムの爆発的な拡大が見込まれる将来、上流工程で生成される情報を再利用した安全なシステムの構築、安全な運用、それらの自動化が望まれる