MITSUBISHI ELECTRIC
Changes for the Better

社外秘

スマート家電における数理モデルを利用した脆弱性評価手法

三菱電機株式会社
設計技術開発センター ソフトウエア技術部 製品セキュリティ技術G
　◯小林大晃　久野倫義　宮内茂人　中込友明　藤原秀治

大阪大学　大学院工学研究科｜機械工学専攻　教授
　澤田賢治

大阪大学　大学院工学研究科　特別研究学生／電気通信大学
　岡村望夢

E-mail：Kobayashi.Hiroaki@bp.MitsubishiElectric.co.jp

三菱電機株式会社

目次

社外秘

- はじめに
- 自己紹介
- 脆弱性評価の課題と狙い
- 脆弱性評価の手順
  - システム仕様の定義
  - 状態遷移表と情報資産の定義
  - 脅威の抽出
  - モデル作成（正常時と脅威発生時）
  - 状態遷移図の生成（正常時と脅威発生時）
  - 脆弱性への対抗策の検討
  - モデル作成（脅威が発生する場合を模擬）
- まとめ

はじめに

- 大学との共同研究において、鉄道模型システムにおける研究を他の領域に拡大できるかを検討している状況を発表する。
- 主な共同研究成果（電気通信大学 澤田賢治先生、岡村望夢氏との共著）
  - IECON2024:
    - On Vulnerability and Robustness Analysis of Railway Control System Using Digital Twin Model
      https://ieeexplore.ieee.org/abstract/document/10905072
  - SCIS2024
    - デジタルツインによる鉄道制御系の脆弱性評価と強靭化の検討
      https://www.iwsec.org/scis/2024/program.html
  - 2024年電気学会電子・情報・システム部門大会
    - デジタルツイン表現による鉄道制御システムの脆弱性解析と強靭化
      https://ieej.bookpark.ne.jp/products/ieej-btc2024tc122006

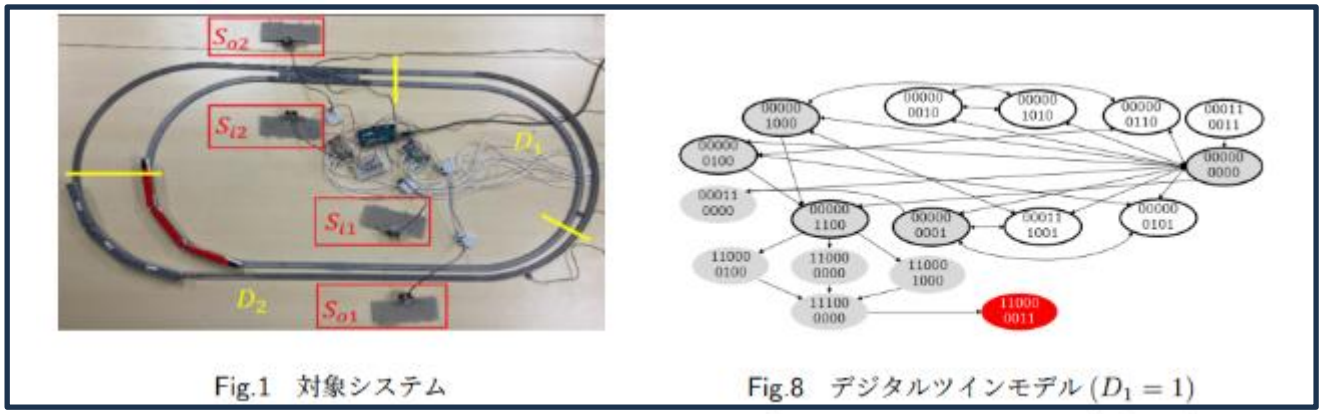


Fig.1 対象システム　　Fig.8 デジタルツインモデル ($D_1 = 1$)

共同研究の鉄道模型システム

自己紹介

社外秘

三菱電機株式会社 設計技術開発センター
ソフトウエア技術部 製品セキュリティ技術G
小林 大晃

経歴

- 2016年　入社 先端技術総合研究所
  車載S/W向けプラットフォームの開発
- 2020年　名古屋製作所
  産業用制御システム向けの国際標準である
  IEC 62443-4-1の認証取得プロジェクトに従事
- 2025年　設計技術開発センター（現職）
  IEC 62443-4-1の認証取得経験を生かし、
  全社の製品セキュリティ強化を推進

私について

名古屋在住で、趣味はカメラです。
週末は家族と過ごすことが多く、家族の大切な瞬間を
写真に収めることを楽しんでいます。

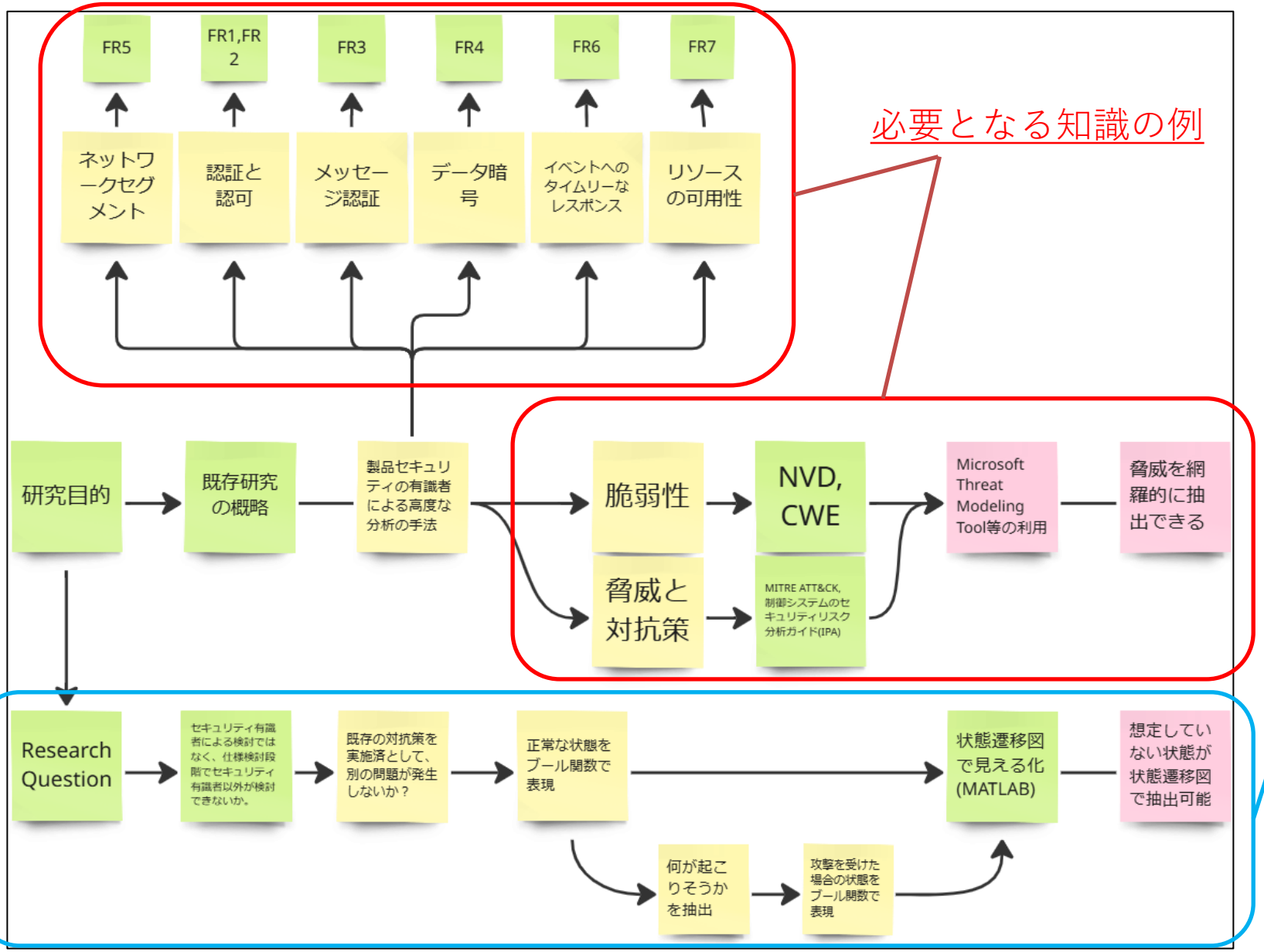
脆弱性評価の課題と狙い（1/2）

社外秘

- 製品仕様を検討する技術者が、セキュリティに対する脆弱性や脅威を把握し適切な対策を検討するには、高度なセキュリティに関する知識を必要とする。
- そのため、製品セキュリティの分析は、セキュリティエキスパートに依存することが多くなり、製品仕様を検討する技術者にとって、ブラックボックスになる危険性がある。
- このような状況を解決するため、製品仕様を検討する技術者が理解しやすく且つ体系的なセキュリティ分析を実施できる手法を提案する。体系的な分析を実現する上で、製品の状態遷移表現にブーリアンネットワークという数理表現を活用することで、既存の脆弱性評価やリスク分析手法の自動化を目指した活動を紹介する。

脆弱性評価の課題と狙い (2/2)

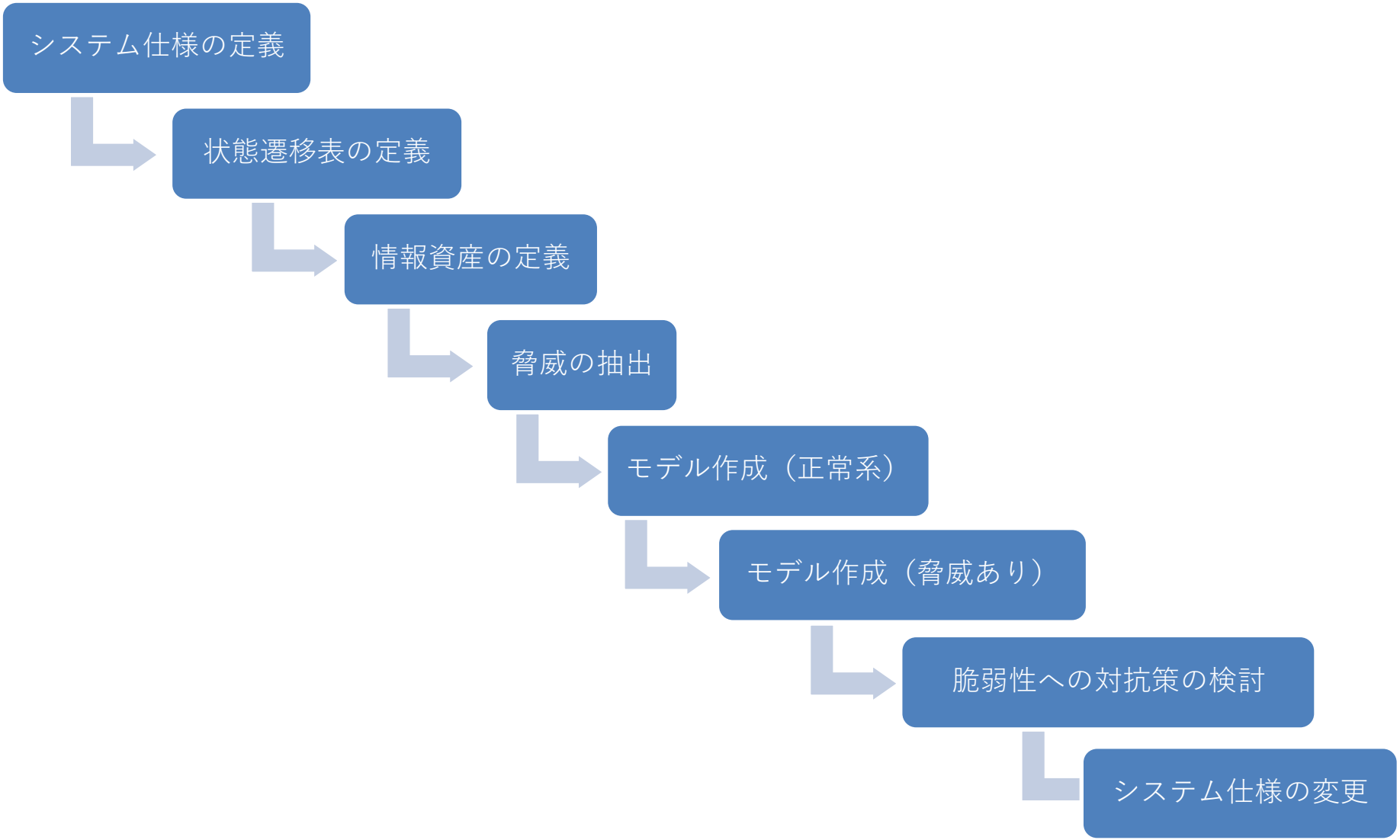
社外秘



脆弱性評価の手順

社外秘

製品仕様を検討する際に必要な状態遷移設計において、数理モデルを利用することで、仕様を検討する技術者が体系的に脆弱性を評価できる。



手順の概要説明

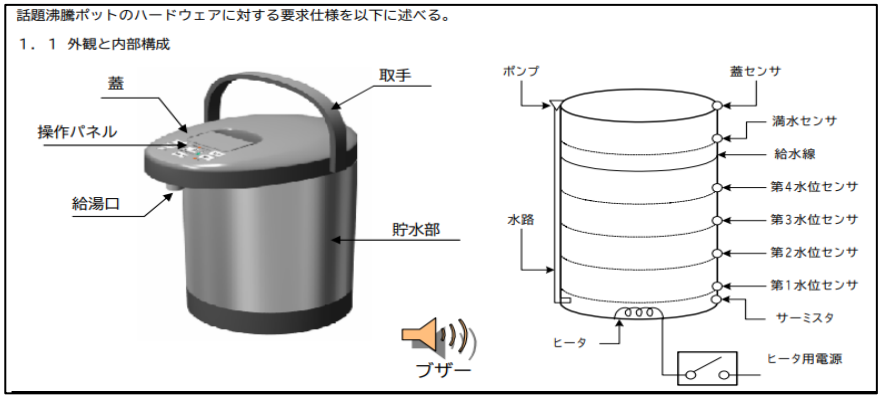
社外秘

No.	手順名	手順概要
1	システム仕様の定義	開発するシステムの仕様、ユースケース、制御仕様、機器構成、ネットワーク構成を整理し、文書化する。
2	状態遷移表の定義	システム仕様から状態遷移表を作成し、仕様として問題ないかを確認する。
3	情報資産の定義	システム仕様から情報資産を洗い出す。
4	脅威の抽出	脅威一覧を利用し、本システムで発生する可能性のある脅威を「脅威の発生可能性と具体的な脅威例」欄へ記載する。
5-1	モデル作成（正常系）	システム仕様、情報資産から状態遷移をブール関数で作成する。
5-2	状態遷移図生成(正常)	ブール関数の情報をプログラムへ組み込み、状態遷移図を生成する。
5-3	状態遷移の評価	生成した状態遷移にて、想定した状態遷移であること、異常な状態がないことを確認する。
6-1	モデル作成(脅威あり)	脅威の抽出で検討した脅威をブール関数に追加する。
6-2	状態遷移図生成(脅威あり)	ブール関数の情報をプログラムへ組込み、状態遷移図を生成する。
6-3	状態遷移の評価（脆弱性の抽出）	生成した状態遷移にて、異常な状態の発生を確認する。 必要であれば、脅威を表現するブール関数を修正（No.6-1）する。 異常な状態がなければ、検討を終了する。
7-1	脆弱性への対抗策検討	No.6にて確認した脆弱性に対する対抗策を検討し、ブール関数へ追加する。
7-2	状態遷移図生成(対抗策あり)	ブール関数の情報をプログラムへ組込み、状態遷移図を生成する。
7-3	状態遷移の評価(対抗策の効果)	生成した状態遷移にて、異常な状態がないことを確認する。
8	システム仕様の変更(必要あれば)	検討した結果に基づき、仕様を見直す。

システム仕様の定義(1/2)

社外秘

■ユースケース概要
電源ON（電源ケーブルをコンセントにつなぐ）
水を入れる
沸騰する
保温する
給湯する
電源OFF（電源ケーブルをコンセントにつなぐ）
スマホからヒータをONにする（オプション機能）
見守り機能（オプション）



組込みシステム教育教材　話題沸騰ポット　GOMA-1015型
要求仕様書　を参考に検討。
https://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm

■仕様
状態　　：アイドル、沸騰、保温
センサー：サーミスタ１つ、水位センサ4つ（第一水位センサOFFなら沸騰要求不可）、
　　満水センサ、蓋センサ（センサOFFなら沸騰要求不可）
ヒータ　：１つ
制御　　：沸騰ボタン及び沸騰要求（制御プログラム）によりヒーターをON。
ボタン　：沸騰、給湯、解除、タイマ（今回考慮しない）

システム仕様の定義(2/2)

社外秘

■基本動作
電源ON⇒水温計測１（サーミスタ）⇒（T＜80°）なら沸騰要求ON⇒水温計測２（サーミスタ）
(T<80°)なら沸騰要求保持
（T>80°）なら沸騰要求OFF⇒水温計測１（サーミスタ）に戻る。

■制御動作
①蓋センサON、第一水位センサON、水温計測1（サーミスタ）ONなら、沸騰要求（制御プログラム）
②蓋センサON、第一水位センサON、沸騰ボタンONなら、沸騰要求
③蓋センサON、解除ボタンON、給湯ボタンON、第1水位センサONなら、給湯
④蓋センサON、第一水位センサONなら解除ボタンON。一定時間（30秒）経過後に解除ボタンをOFFにする
⑤空焚きを避ける＝蓋が開いた、水がない場合、沸騰要求をOFF、沸騰ボタンを押せない、ヒータをオフする。
⑥沸騰要求、沸騰ボタンが押されたら、ヒーターがONになる
⑦蓋が開けられたら、その後蓋は閉じられる。
⑧外部入力（a2,a3,a4,s3）のONが維持されるかどうかに判断（s3：水有のみ維持される）

■ネットワーク関連動作
①追加機能（宅外からお湯を沸かせる）のため、ネットワークへ接続する。
②スマートフォンにインストールした専用アプリからWi-Fi を経由し、コマンドを受信。
③コマンドにより、沸騰要求・沸騰停止を実行する。
④受け付けたコマンドに対し、成功／失敗をWi-Fi経由でスマホへ送信する。

状態遷移表と情報資産の定義

社外秘

状態遷移表

現在の状態	イベント	次の状態	アクション
アイドル	蓋センサon	沸騰行為	沸騰開始
アイドル	沸騰ボタン押下	沸騰行為	沸騰開始
アイドル	保温ボタン押下	保温行為	保温開始
アイドル	エラー検知	エラー	エラー処理
沸騰行為	沸騰完了	保温行為	保温開始
沸騰行為	エラー検知	エラー	エラー処理
保温行為	保温完了	アイドル	なし
保温行為	エラー検知	エラー	エラー処理
エラー	なし	エラー	なし

組込みシステム教育教材　話題
沸騰ポット　GOMA-1015型 要求仕様書　を参考に検討。
https://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm

情報資産

No.	情報資産
1	電気ポット本体プログラム
2	オペレーティングシステム
3	ポット利用ログ

脅威の抽出（1/4）

社外秘

■脅威一覧（IPA「制御システムのセキュリティリスク分析ガイド第２版」等を参考に作成）を用いて、本システムにおける発生可能性を検討する。

IPA「制御システムのセキュリティリスク分析ガイド第２版」より検討（22個の脅威がある）

IEC 62443、米国国防省のサイバーセキュリティのフレームワークより検討

対象製品で脅威が発生するかを検討

	脅威の中区分				対抗策の区分					検討に使用する欄	
脅威の大区分	手法に関する脅威（侵入系）	手法に関する脅威（実行系）	被害内容に関する脅威	Faundational Requirments（IEC 62443）の対応	予防・防止	検知・追跡	回復	抑止・抑制（人の意識に対するもの）	備考	脅威の発生可能性（○△×）	具体的な脅威例
資産（機器）に対して想定される脅威	不正アクセス			FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 5 データフロー制御 FR 6 イベントへのタイムリーなレスポンス	FR1 FR2 FR3 FR5	FR6			FR3とFR5は不正アクセスが成功した後に他の脅威が発生した場合の対抗策 ・認証 ・アカウントの管理 ・アクセス制御 ・監査証跡の生成と管理 ・入力検証 ・ネットワークの分離 ・侵入検知	○	・スマホアプリを経由してへアクセス。 ・宅内Wi-Fiを利用してへアクセス。
	物理的侵入			FR 1 識別及び認証管理（アクセス制御）	FR1				FR6については必要に応じて検討。	×	なし
		不正操作		FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御	FR1 FR2				FR6については必要に応じて検討。 ・認証 ・アカウントの管理 ・アクセス制御	○	沸騰要求を常時ONさせる。
		過失操作		FR 1 識別及び認証管理（アクセス制御）	FR1				FR2については必要に応じて検討。 ・システム利用通知	×	元の仕様にて考慮している。
		（機器への）不正媒体・機器接続		FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 6 イベントへのタイムリーなレスポンス	FR1 FR2	FR6			・認証 ・無線通信のセキュリティ ・アクセス制御 ・無線通信のセキュリティ ・デバッグポート保護 ・監査証跡の生成と管理	×	USBなどの不正機器接続の可能性はあるが、今回は考慮しない。
		プロセス不正実行		FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 6 イベントへのタイムリーなレスポンス	FR1 FR2 FR3	FR6			不正アクセスに続きプロセス不正実行 ・認証 ・アカウントの管理 ・アクセス制御 ・監査証跡の生成と管理 ・デバッグポート保護 ・不正プログラムからの保護 ・監査証跡の生成と管理	×	現時点ではなし。

脅威の抽出（2/4）

社外秘

	脅威の中区分				対抗策の区分					検討に使用する欄	
脅威の大区分	手法に関する脅威（侵入系）	手法に関する脅威（実行系）	被害内容に関する脅威	Fundamental Requirments（IEC 62443）の対応	予防・防止	検知・追跡	回復	抑止・抑制（人の意識に対するもの）	備考	脅威の発生可能性（○△×）	具体的な脅威例
		マルウェア感染		FR 3 システムの完全性 FR 6 イベントへのタイムリーなレスポンス	FR3	FR3 FR6	FR3		FR3システムの完全性でマルウェアからの影響を防止・検出・報告及び軽減する仕組みを有することを求めている。 ・不正プログラムからの保護 ・入力検証 ・プログラムのアップデート ・ブートの完全性 ・セキュリティ自己診断 ・ソフトウェアと情報の改ざん防止 ・信頼の基点 ・監査証跡の生成と管理	×	OSがある可能性はあるが、マルウェア感染の可能性は低いと判断。
			情報窃取	FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 4 データの機密性 FR 6 イベントへのタイムリーなレスポンス	FR1 FR2 FR3 FR4	FR6			・認証 ・アカウントの管理 ・アクセス制御 ・監査証跡の生成と管理 ・セッション管理 ・デバッグポート保護 ・暗号と鍵管理 ・耐タンパー ・ソフトウェアと情報の改ざん防止 ・暗号と鍵管理 ・監査証跡の生成と管理	○	電気ポット本体プログラムの窃取。 ポット利用ログにより、生活パターンが窃取される。
			情報改ざん	FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 4 データの機密性 FR 6 イベントへのタイムリーなレスポンス FR 7 リソースの可用性	FR1 FR2 FR3 FR4 FR7	FR6	FR7		・認証 ・アカウントの管理 ・アクセス制御 ・監査証跡の生成と管理 ・セッション管理 ・デバッグポート保護 ・暗号と鍵管理 ・耐タンパー ・ソフトウェアと情報の改ざん防止 ・暗号と鍵管理 ・監査証跡の生成と管理 ・バックアップ/リストア	○	電気ポット本体プログラムの改ざん
			情報破壊	FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 6 イベントへのタイムリーなレスポンス FR 7 リソースの可用性	FR1 FR2 FR3 FR7	FR6	FR7		・認証 ・アカウントの管理 ・アクセス制御 ・監査証跡の生成と管理デバッグポート保護 ・暗号と鍵管理 ・耐タンパー ・ソフトウェアと情報の改ざん防止 ・監査証跡の生成と管理 ・バックアップ/リストア	○	電気ポット本体プログラムの削除
		不正送信		FR 2 使用制御 FR 3 システムの完全性 FR 5 データフロー制御 FR 6 イベントへのタイムリーなレスポンス	FR2 FR3 FR5	FR6			・監査証跡の生成と管理 ・暗号と鍵管理 ・デバッグポート保護 ・不正プログラムからの保護 ・ネットワークの分離 ・監査証跡の生成と管理	○	不正コマンドの送信

脅威の抽出（3/4）

社外秘

	脅威の中区分				対抗策の区分					検討に使用する欄	
脅威の大区分	手法に関する脅威（侵入系）	手法に関する脅威（実行系）	被害内容に関する脅威	Fundamental Requirments（IEC 62443）の対応	予防・防止	検知・追跡	回復	抑止・抑制（人の意識に対するもの）	備考	脅威の発生可能性（○△×）	具体的な脅威例
			機能停止	FR 3 システムの完全性 FR 5 データフロー制御 FR 6 イベントへのタイムリーなレスポンス	FR3 FR5	FR6			・出力制御 ・プログラムのアップデート ・ソフトウェアと情報の改ざん防止 ・ネットワークの分離 ・監査証跡の生成と管理	○	沸騰解除機能の停止
			制御不能・異常動作（IPA資料第2版にて追加）	FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 3 システムの完全性 FR 5 データフロー制御 FR 6 イベントへのタイムリーなレスポンス FR 7 リソースの可用性		FR6	FR7			○	沸騰状態の継続による空焚きの発生
			高負荷攻撃	FR 5 データフロー制御 FR 7 リソースの可用性	FR5 FR7		FR7		FR6については必要に応じて検討。 ・ネットワークの分離 ・DoS攻撃対策 ・資源管理	×	ICMP攻撃などの可能性はあるが、正規のプロセスの不正実行は考慮しない。
		窃盗		FR 1 識別及び認証管理（アクセス制御）	FR1				・物理的な窃盗	×	今回は考慮しない。
			盗難・廃棄時の分解による情報窃取	FR 4 データの機密性	FR4				・暗号と鍵管理 ・データの消去	×	プログラム自体の窃取
資産（通信経路）に対して想定される脅威		経路遮断		FR 6 イベントへのタイムリーなレスポンス	FR7	FR6	FR7		・監査証跡の生成と管理 ・侵入検知	×	無線通信の妨害の可能性はあるが、今回は考慮しない。
		通信輻輳		FR 5 データフロー制御 FR 6 イベントへのタイムリーなレスポンス	FR5 FR7	FR6	FR7		・ネットワークの分離 ・監査証跡の生成と管理 ・侵入検知	×	無線通信の妨害の可能性はあるが、今回は考慮しない。
		無線妨害		FR 2 使用制御 FR 6 イベントへのタイムリーなレスポンス	FR2 FR7	FR6	FR7		・無線通信のセキュリティ ・監査証跡の生成と管理 ・侵入検知	×	無線通信の妨害の可能性はあるが、今回は考慮しない。
			盗聴	FR 4 データの機密性 FR 5 データフロー制御	FR4 FR5				・暗号化通信 ・ネットワークの分離	×	なし
			通信データ改ざん	FR 3 システムの完全性 FR 6 イベントへのタイムリーなレスポンス	FR3	FR6			・暗号化通信 ・監査証跡の生成と管理 ・侵入検知	×	無線通信の妨害の可能性はあるが、今回は考慮しない。
		不正機器接続		FR 1 識別及び認証管理（アクセス制御） FR 2 使用制御 FR 6 イベントへのタイムリーなレスポンス	FR1 FR2	FR6			・認証 ・監査証跡の生成と管理 ・デバッグポート保護 ・監査証跡の生成と管理 ・侵入検知	×	経路上で不正機器の接続は考慮しない。

脅威の抽出（4/4）

■脅威（脅威一覧表で〇になった脅威を深掘りする）
宅内無線LANへ不正アクセスし、
不正操作、プロセス不正実行、不正送信を実行し、制御不能・異常動作を発生させる。

⇒無線LANにおける不正アクセスの防止対抗策にて実施することで防止できる？
⇒無線LAN経由でアクセス可能となり、不正コマンドを送付された場合、どうなる？
⇒状態遷移における問題を検討してみる。

組込みシステム教育教材　話題沸騰ポット　GOMA-1015型 要求仕様書　を参照し検討。
https://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm

モデル作成（まずは正常動作）

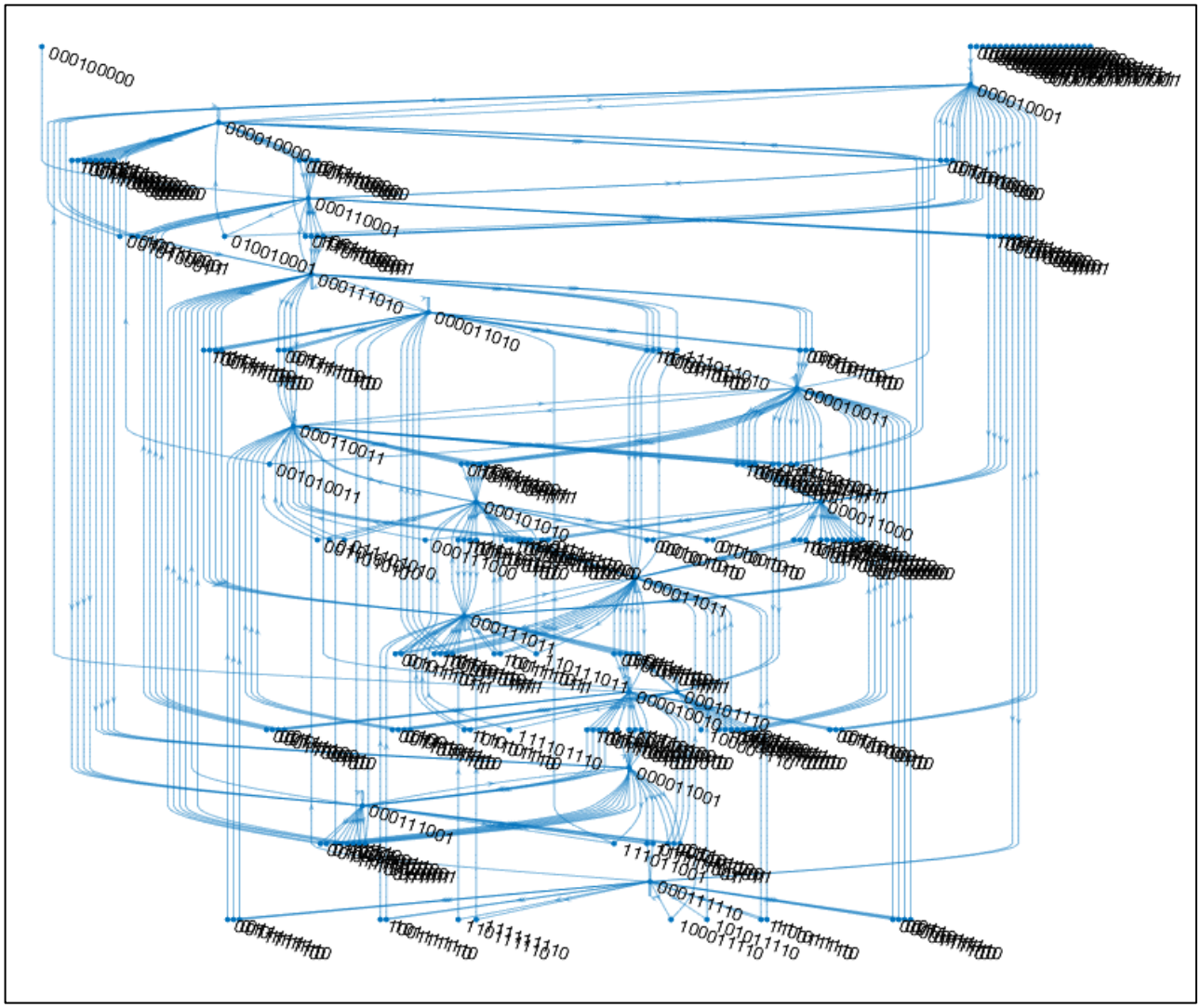
社外秘

■ 基本方針：センサーの情報は外部入力とし、外部入力により制御が変化する。
■ 変数の定義：下記変数で下線の変数のみをブール関数で定義した（状態遷移に関わる部分のみを対象）
s1:電源、**s2:サーミスタ（T<80° でON）**
s3:第1水位センサでポットの最下位置のセンサ、s4:第2水位センサ、s5:第3水位センサ
s6:第4水位センサ：ポットの最上位置のセンサ、s7:満水センサ、**s8:蓋センサ**
a1:沸騰要求ON／OFF
a2:沸騰ボタン（沸騰要求ON／OFF）
a3:解除ボタンON/OFF
a4:給湯ボタンON/OFF
a5:給湯ON/OFF
h:ヒーターON/OFF

■ブール関数・・・f(k+1) = g(k)の意味は、gがONになると次にfがONになることを意味する。
a1(k+1)=(s2(k) ∧ s3(k) ∧ s8(k)) ∨ a2(k)・（温度が80° 未満、水があり、蓋が閉まっている）又は沸騰ボタンがONなら沸騰要求が発生する。
a5(k+1)=s8(k) ∧ a3(k) ∧ a4(k) ∧ s3(k)・蓋が閉まり、解除ボタンが押され、給湯ボタンが押され、水があれば、給湯できる。
s2(k+1)=¬s3(k) ∨ ¬s8(k) ∨ ¬h(k)・水がなく、蓋が開いていて、ヒータOFFなら温度が下がる
h(k+1)=(s2(k) ∧ s3(k) ∧ s8(k)) ∨ a1(k)・（温度が80° 未満、水があり、蓋が閉まっている）又は沸騰要求がONならヒータがONになる。
s8(k+1)=¬s8(k)・蓋が開いたままの状態にはならない。
a2_next = a2 * 0・沸騰ボタンが1度押されるが、次には解除される。
a3_next = a3 * 0・解除ボタンが1度押されるが、次には解除される。
a4_next = a4 * 0・給湯ボタンが押されるが、ボタンを離すと解除される。
s3_next = s3 ・水がなくなった状態は継続する。

状態遷移図（正常動作をMATLABで自動生成）

各ビットが前頁に定義した変数[a2, a3, a4, s3, s2, a1, a5, h, s8] の状態を表す。
複雑な遷移ですが、（目視にて）正常な状態であることを確認した。



モデル作成（脅威が発生する場合を模擬）

社外秘

■ブール関数・・・f(k+1) = g(k)の意味は、gがONになると次にfがONになることを意味する。

a1(k+1)=(s2(k)∧s3(k)∧s8(k)) ∨ a2(k) ∨ ~a1(k) ∨ a1(k) ・・・a1が常にオンにさせられる

a5(k+1)=s8(k)∧a3(k)∧a4(k)∧s3(k)・蓋が閉まり、解除ボタンが押され、給湯ボタンが押され、水があれば、給湯できる。

s2(k+1)=¬s3(k)∨¬s8(k)∨¬h(k)・水がなく、蓋が開いていて、ヒータOFFなら温度が下がる

h(k+1)=(s2(k)∧s3(k)∧s8(k)) ∨ a1(k)・（温度が80°未満、水があり、蓋が閉まっている）又は沸騰要求がONならヒータがONになる。

s8(k+1)=¬s8(k)・蓋が開いたままの状態にはならない。

a2_next = a2 * 0・沸騰ボタンが1度押されるが、次には解除される。

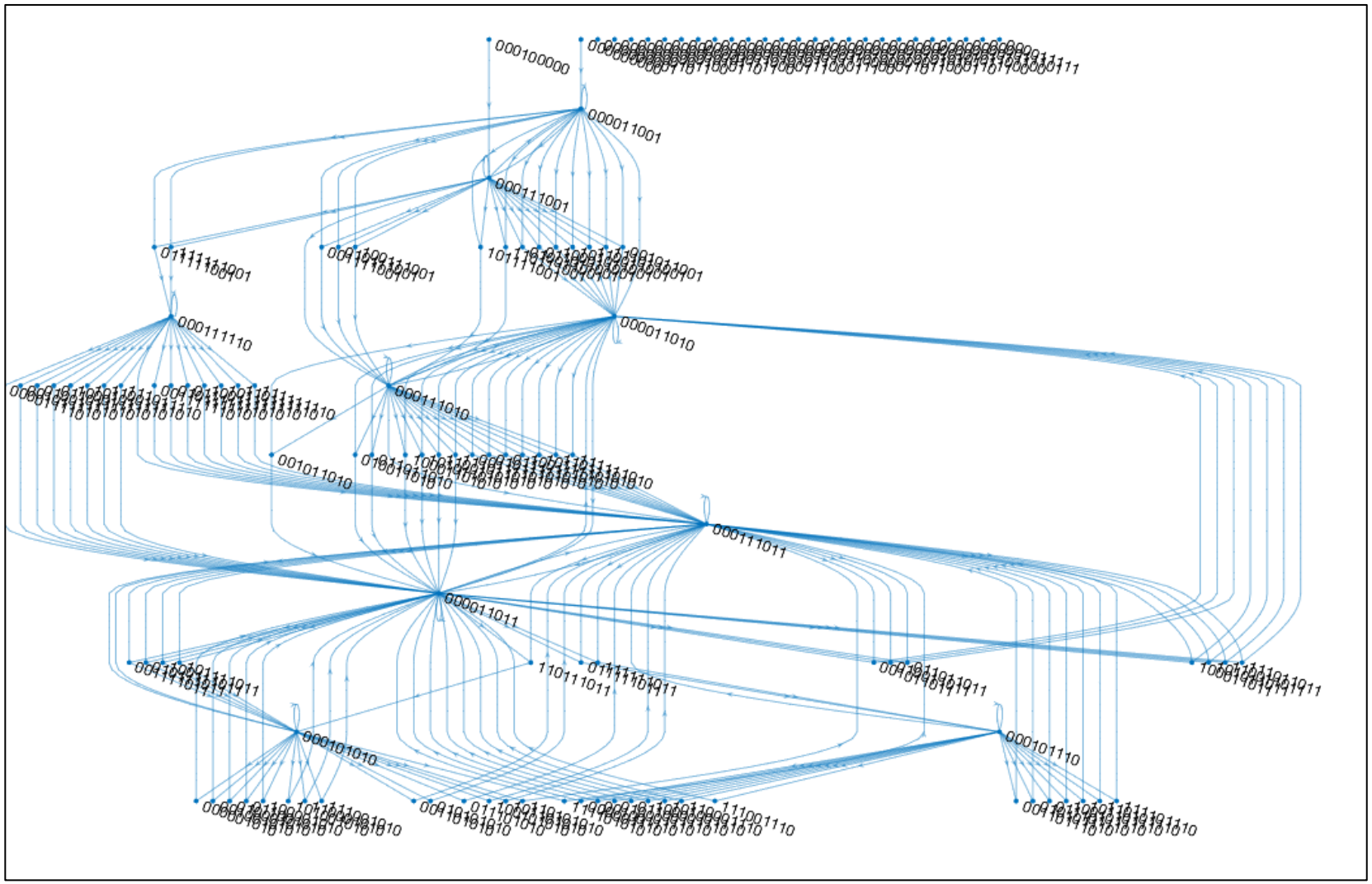
a3_next = a3 * 0・解除ボタンが1度押されるが、次には解除される。

a4_next = a4 * 0・給湯ボタンが押されるが、ボタンを離すと解除される。

s3_next = s3 ・水がなくなった状態は継続する。

状態遷移図（脅威が発生した場合をMATLABで自動生成）

各ビットが前頁に定義した変数[a2, a3, a4, s3, s2, a1, a5, h, s8] の状態を表す。
複雑な遷移ですが、（目視にて）ヒータが連続してONとなる遷移を確認した。



脆弱性への対抗策の検討

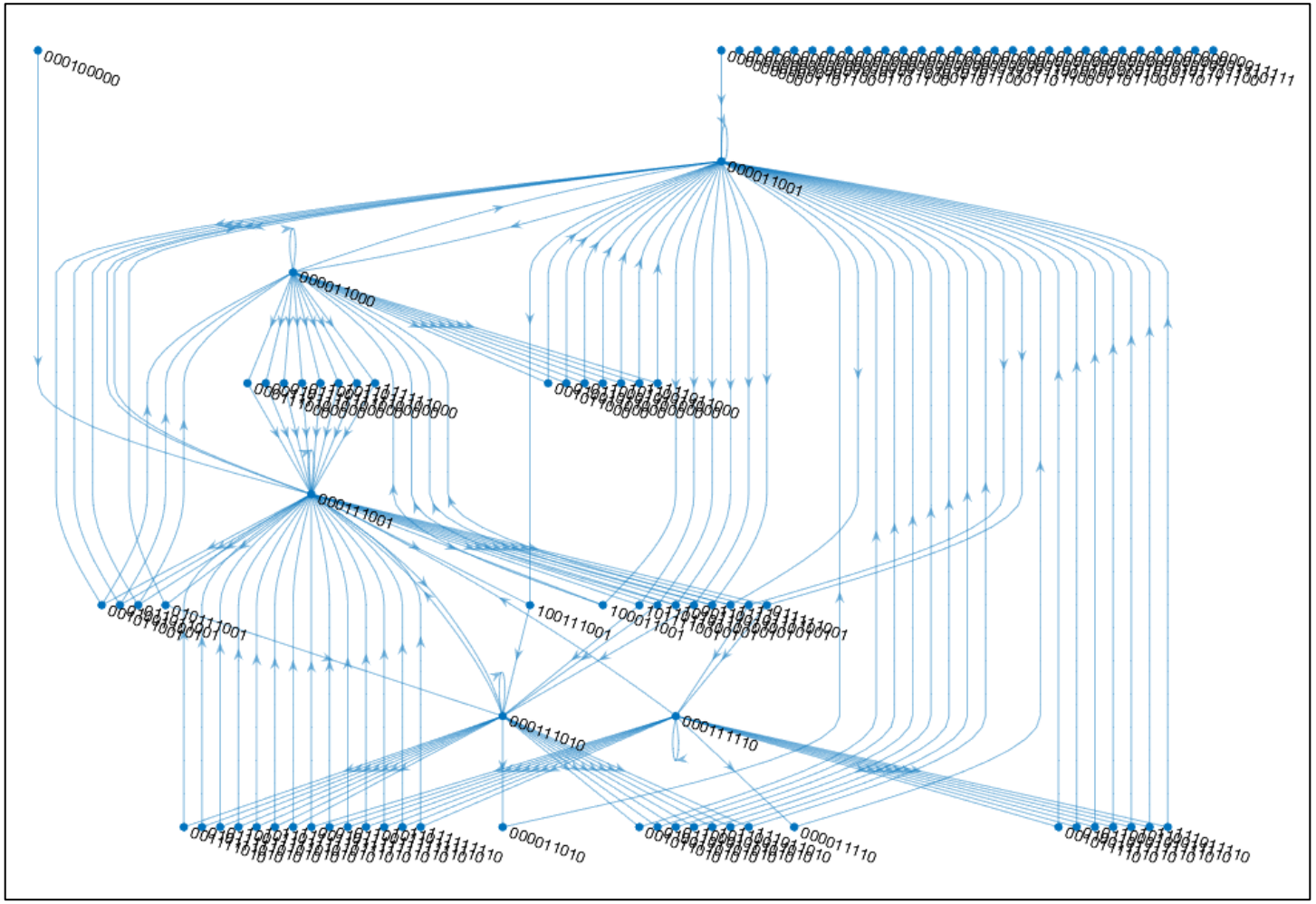
社外秘

■ブール関数・・・f(k+1) = g(k)の意味は、gがONになると次にfがONになることを意味する。

a1(k+1)=(s2(k)∧s3(k)∧s8(k)) ∨ a2(k) ∨ ~a1(k) ∨ a1(k) ・・・a1が常にオンにさせられる
a5(k+1)=s8(k)∧a3(k)∧a4(k)∧s3(k)・蓋が閉まり、解除ボタンが押され、給湯ボタンが押され、水があれば、給湯できる。
s2(k+1)=¬s3(k)∨¬s8(k)∨¬h(k)・水がなく、蓋が開いていて、ヒータOFFなら温度が下がる。
h(k+1)=(s2(k)∧s3(k)∧s8(k)) ∨ ~~**a1(k)**~~ **(s2 ∧ s3 ∧ s8 ∧ a1)・・・a1が単独でONでも他の条件が揃わないとヒータがONにならないように修正**
s8(k+1)=¬s8(k)・蓋が開いたままの状態にはならない。
a2_next = a2 * 0・沸騰ボタンが1度押されるが、次には解除される。
a3_next = a3 * 0・解除ボタンが1度押されるが、次には解除される。
a4_next = a4 * 0・給湯ボタンが押されるが、ボタンを離すと解除される。
s3_next = s3 ・水がなくなった状態は継続する。

状態遷移図（対抗策を挿入した場合をMATLABで自動生成）

各ビットが前頁に定義した変数[a2, a3, a4, s3, s2, a1, a5, h, s8] の状態を表す。
複雑な遷移ですが、（目視にて）ヒータが連続ONとなる遷移がないことを確認した。
結論として、ヒータをONする条件を追加することで、脅威に対応できると結論付けた。



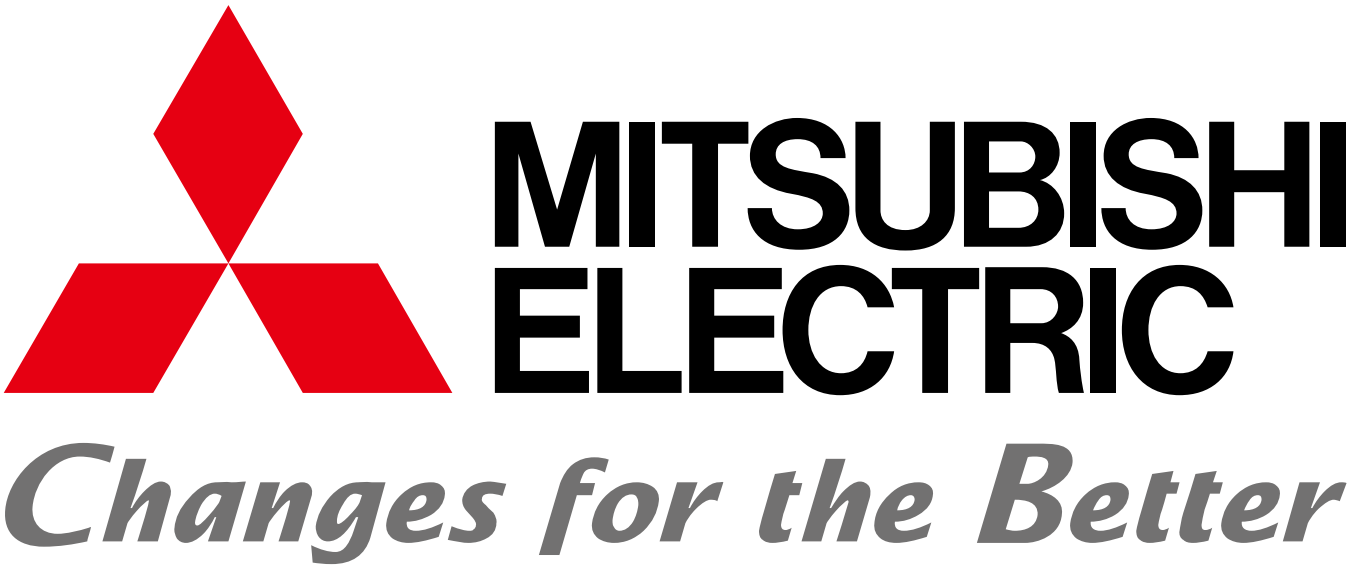
まとめ

■ スマート家電（電気ポット）の製品仕様の検討段階において、外部からの攻撃に対し、脆弱な状態になる可能性を状態遷移図で見える化し、攻撃が発生しても脆弱な状態を発生させない分析手法を定義できた。具体的な工夫点は下記のとおりである。

- 情報処理推進機構が公開している「制御システムのセキュリティリスク分析ガイド」における『資産（機器）に対する脅威（攻撃手法）』等の公開情報を組み合わせて、脅威の抽出方法を定義できた。
- ブーリアンネットワークによるスマート家電の数理モデル化と、数理モデルをインプットとした状態遷移図（MATLABによる自動生成 ）の生成による脆弱性の見える化を実現できた。
- 上記組み合わせによる脅威シナリオを定義し、対抗策の有効性を評価できた。

■ 残された課題

①今回の主な結果が脆弱な状態の見える化であることから、脆弱な状態を検出することは人手に頼る状態になっている。残された課題は、ブーリアンネットワークの特徴を活かした数理手法を用いることで、脆弱な状態を自動で見つけることである。
②ポットを例に手法の定義ができたので、別の製品にて手法の有効性を評価したい。


MITSUBISHI
ELECTRIC
Changes for the Better