様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１９　日現在

機関番号：　１２６１２
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ０６１３４

研究課題名（和文）事象駆動型量子化制御に基づく通信制御系の縮退運転アルゴリズム

研究課題名（英文）Event triggered fallback algorithm for networked systems via quantized control

研究代表者

澤田　賢治（Sawada, Kenji）

電気通信大学・ｉ－パワードエネルギー・システム研究センター・准教授

研究者番号：８０５５０９４６

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：重要インフラの制御系のネットワーク化（通信制御系化）が進む中，制御系のサイバーセキュリティ対策は急務となっている．本研究は通信制御系へのサイバー攻撃対策技術としてモデルベース縮退運転システムを与えた．情報セキュリティ技術を基軸とした従来研究とは違い，「攻撃時でも制御系の基本的な稼働を保証する」可用性を主軸としている．これを実現するために，研究成果として，事象駆動型の量子化制御の提案，制御プログラムのフローグラフの検証，攻撃レベルと検知精度に基づく縮退動作，実装形式と検知精度の関係を得ることが出来た．

研究成果の概要（英文）：Control systems such as critical infrastructures have to be networked due to the flexibility and the efficiency, and this situation causes new threats “cyber-attacks” against control systems. This study proposed the model-based fallback control system that guarantees the continuous operation of the system during the cyber-attacks. The study focuses on the “availability” and the incident response of control system, while the information security focus on the confidentiality. To realize the fallback control system theory, the following results are obtained: event triggered control of quantized system, model checking of program control flow graph, fallback operation depending on the attacking level and the detection accuracy, the relationship between the implementation style and the detection accuracy.

研究分野：　制御システムセキュリティ

キーワード：　制御工学　セキュリテイ　縮退運転システム　事象駆動システム

１．研究開始当初の背景

現在，電気・ガス・水道など生活を支える重要インフラの制御系はネットワーク化（通信制御系化）が進んでいる．ネットワーク化により，発電所や工場等のプラント動作を監視・制御する制御系に対するサイバー攻撃が出現し，大きな社会問題になっている．1990年代後半の米国重要インフラに対する攻撃から始まり，2010年のイラン核燃料施設のウラン濃縮用遠心分離器を標的とした Stuxnet によるサイバー攻撃にまで至っている．制御系のサイバーセキュリティ技術開発は対策急務であり，近年は情報系セキュリティ技術の転用やサイバー攻撃の検知に関する研究が活発である．

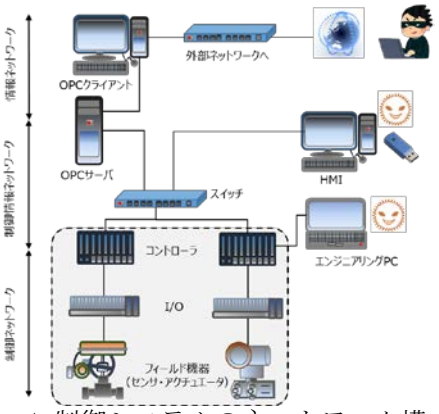

Fig. 1 制御システムのネットワーク構成

一方，通信制御系のセキュリティ担保には，情報系の強化や攻撃検知の高速化を促進すれば良いというわけではない．例として Fig.1 に FA(Factory Automation)システムの通信制御系の階層構造を示す．階層毎の通信プロトコルや通信性能は異なり，これにより各階層のセキュリティ仕様も異なる．特に重要なのは，サイバー攻撃時の制御器系の可用性，すなわちシステムの継続的稼働性能の保証である．制御器系の急激な停止は安全面上の大きな問題であるため，サイバー攻撃時でも PLC（Programmable Logic Controller）はフィールド機器の基本的な機能を保証しつつ稼働し続けなければならない．サイバー攻撃によって基本的な機能を保証できない程の通信逼迫や切断が生じた場合，通信制御系は機能を制限し制御性能を劣化させても稼働し続ける（縮退運転）ことが求められる．このように，通信御御系ではサイバー攻撃時の可用性や縮退運転に着目した制御理論・技術が必須であるが，未だ確立されていない．

２．研究の目的

本研究は通信制御系へのサイバー攻撃に対して，縮退運転という形で対策技術を開発することを目的とした．これまでのサイバーセキュリティ対策が情報セキュリティ技術の転用に留まる中，制御系の可用性を主眼に「攻撃時でも制御系の基本的な稼働を保証する」ことが本研究の特色である．これを実現する上で，本研究では事象駆動型の新しい量子化制御をベースに，攻撃時の性能劣化レベルを補償した通信制御系の縮退運転アルゴリズムを研究開発することを目指した．具体的には，上記を実現するために，**事象駆動型の縮退運転手法の確立**，**制御プログラムのフローグラフの検証方法の提案**，**攻撃レベルと検知精度に基づく縮退動作の実現**，さらに，**実装形式と検知精度の関係の明確化**を目指した．

これまで事象駆動型の制御アルゴリズムの学術研究は，通信速度の変化に着目して研究が行われてきた．特にネットワーク経由の制御対象を安定化できる範囲での通信速度に特化している．これに対して，本研究課題は性能劣化レベルを補償した量子化レベルと通信速度の変化に焦点を当てており，既存の事象駆動型制御の発展系となっている．

当該分野における本研究の学術的な特色・独創的な点・結果の意義として，まず，通信制御系のサイバーセキュリティにおいて可用性と縮退運転に着目したことにある．特に縮退運転アルゴリズムを量子化制御の観点から与えることは学術面・応用面の両方から独創的である．また，量子化レベルと通信速度の可変化を事象駆動型で実現する点にも特色がある．本研究課題による成果によって，性能劣化レベルを補償した縮退運転アルゴリズムの基礎を提供した．また，実機実験による検証によって，縮退運転アルゴリズムに必要な制御器性能の知見を与えた．

３．研究の方法

本研究の目的“事象駆動型量子化制御に基づく通信制御系の縮退運転アルゴリズム”を達成するため，つぎの三課題を設定した．第一に，量子化を考慮した事象駆動型の量子化制御（平成 27 年度）である．この課題では**事象駆動型の縮退運転手法の基礎の確立**，**制御プログラムのフローグラフの検証方法の提案**を目指した．第二に，量子化レベルと通信速度変化に着目した事象駆動型の量子化制御（平成 28，29 年度）である．本課題では，平成 27 年度で得られた成果の拡張に加えて，**攻撃レベルと検知精度に基づく縮退動作の実現**を目指した．第三に縮退運転アルゴリズムの実機検証（平成 28，29 年度）である．提案アルゴリズムを PLC へ適用することで，事象駆動型量子化制御に必要なマイコンの演算性能を明らかにし，アルゴリズムの高速化や簡易化手法について研究を行った．すなわち，**実装形式と検知精度の関係の明確化**を目指した．以降，詳細について述べる．

（1）量子化を考慮した事象駆動型の量子化制御（平成 27 年度）

① **不変集合解析に基づく事象評価：**事象駆動型の通信制御では，制御対象への制御入力の更新タイミングは通信周期に非同期である．通信非同期を考慮したシス

テムの安定性と事象駆動の制御性能の関係をリアプノフ関数と不変集合解析から明らかにする．

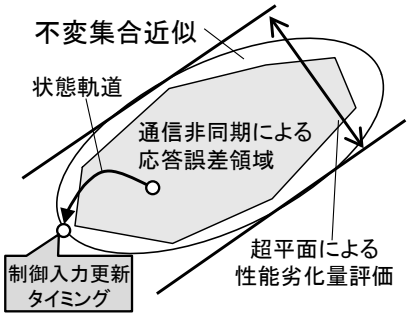

Fig. 2 事象評価と制御則更

② **量子化要素がある系の事象駆動型制御**：Fig.2 において，量子化要素による応答誤差領域を考慮し，それによる性能劣化レベルを超平面により評価する．本手法を LMI（線形行列不等式）に基づく効率的な制御アルゴリズムの形で導出する．

③ **制御器設計と事象評価の統合**：項目 2 の事象評価アルゴリズムを通信制御系の制御器の設計条件にも適用できるように拡張する．設計条件の複雑化を回避するため，制御器構造は状態フィードバックゲインに限定する．

(2) 量子化レベルと通信速度変化に着目した事象駆動型の量子化制御(平成 28,29 年度)

① **事象駆動型に基づく通信速度と量子化レベルの可変化**：通信速度の変化（サイバー攻撃の変化）に応じた量子化レベルの変化（縮退動作の変化）のモデル化方法と解析方法を与える．

② **通信速度，量子化レベルと制御器の同時最適化**：通信速度，量子化レベルの可変化と制御器の設計条件を与える．設計条件の複雑化を回避するため，制御器構造は状態フィードバックかつ定数ゲインに限定する．

③ **サンプル値制御系への拡張**：縮退運転アルゴリズムを実機に適用するために，サンプル値系（制御対象：連続系，制御器：離散系）を考える．

(3) 縮退運転アルゴリズムの実機検証

実機検証では，縮退運転アルゴリズムとしての事象駆動型量子化制御に**必要な演算性能を明らかにし，同アルゴリズムの高速化や簡易化手法**について研究を行う．また，高速化と劣化性能補償のトレードオフ性の実機検証も行う．組込コントローラとして Arduino を利用し，アルゴリズム実装に Mathworks 社の CAD ソフト Matlab/Simulink を利用する．それに加え，PLC への縮退運転アルゴリズムの実装を行う．

４．研究成果

(1)平成 27 年度

事象駆動型の縮退運転手法と制御プログラムのフローグラフの検証方法に関して以下の成果が得られた．

①ネットワークの逼迫情状況を想定した性能劣化抑制手法

サイバー攻撃時にネットワークの送信レートが低下し，アクチュエータ送信信号・センサー受信信号の解像度が劣化する状況を想定した制御手法を与えた．制御系の構造として，状態フィードバック制御(発表[13])，動的量子化器制御（論文[9])，出力フィードバック制御（発表[9]）を考慮したものを与えた．サンプル値制御とモデル追従制御を考慮することで，最低限保証したい制御性能を陽に考慮出来るようになった．制御系の複雑度も考慮し，動的制御器の低次元化にまで踏み込んでいる．具体的には，低次元化により性能が劣化する場合と劣化しない場合の設計手法を凸最適化問題のクラスで与えている（発表[14]).

②ネットワーク上のサイバー攻撃を制御対象側のアクチュエータ・センサ信号値から検出する方法

既存のサイバー攻撃検知手法がネットワーク上の信号を使うのに対して，本成果ではネットワーク信号を使わない方法を与えている（発表[11,12,14]）．外乱オブザーバに基づく方法と切換型リアプノフ関数に基づく方法を与え，実機実験（Fig. 3）で有効性を検証している．その上で，攻撃検知後に制御システムも防御モードに切り替える機構を組込コントローラ（Arduino）で実現している．

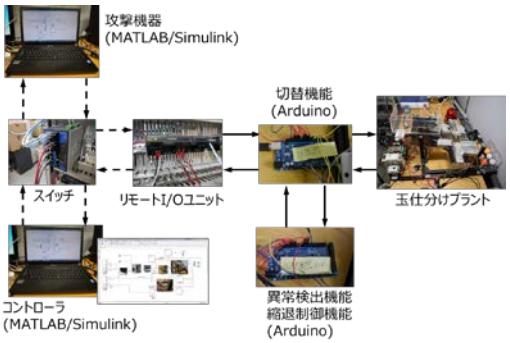

Fig. 3 実機検証環境

③フローグラフに着目したプログラム改竄検出手法

制御プログラムのフローグラフを離散事象システムとして捉え，ペトリネットによるモデル化と状態方程式化を扱った．プログラムが状態方程式化することで，プログラム改竄が可制御・不可制御・可観測・不可観測空間の変更に帰着される．すなわち，カルマン正準分解により制御システムのプログラム改竄を特徴付けることができるようになった（発表[10]).

④当該年度の研究成果に対する自己評価

当該年度は理論構築と実機実験を平行して進めることができた．理論構築では，サンプル値制御，モデル追従制御，量子化制御を融合深化することが出来ていて，学術的な新規性を高めることが出来た．また，実機実験では，サイバー攻撃の実体に沿った攻撃例（中間者攻撃）に対して，提案する縮退運転アルゴリズムが功を奏することを明らかにした．実機実装に関して当初の計画以上に進展することができた．

(2)平成 28 年度

本年度は攻撃レベルと検知精度に基づく縮退動作の実現に関わる成果が主結果であるが，実装形式と検知精度の関係の明確化に関わる研究成果も得られた．

①制御システムの状態遷移を離散事象システムでモデル化し，サイバー攻撃による状態異常を検出する方法

モデル化対象は制御システム内のフィールド機器とコントローラの 2 つを考慮した．離散事象システムに基づくオブザーバを効率的に適用するために，モデルの低次元化をカルマン正準分解の観点から与えた．また，複数の異常検出器が制御系内に介在するとき，異常検出の競合を避けるため，中間者攻撃が存在する状況でのネットワークを介した協調型状態推定方法も与えた．また，制御システムのライフサイクルを考慮した防御技術では，保守運転から通常運転への復帰プロセスを考慮した異常検出器の構築が可能となった．

②制御プログラムの更新解析

プログラム（C 言語ソースをコンパイル時に発生する制御フローグラフ）に対してカルマン正準分解を適用することで，プログラムの安全更新解析の基礎を与えた．同手法では，タスクの静的な実行順序表現をペトリネットにより動的な実行順序表現に変換している．これにより，システムの遷移状態によっては実行されないタスクを洗い出し，正規コマンドの乗っ取りや改ざんに流用されないように無駄なスクリプトの削除に貢献できるものとなっている（発表[8]）．

③コントローラにおけるもベルベース型異常検出

Programmable Logic Controller を対象に，制御機器用のプログラミング言語で実装可能なモデルベース型異常検出方法の基礎設計方法をペトリネットから考慮した．結果として，フィールド機器の実行順序を踏まえたペトリネットかプログラミング言語への変換方法を与えた．

④当該年度の研究成果に対する自己評価

提案する縮退運転アルゴリズムは，中間者攻撃に加えて DoS 攻撃やプログラム改変への対応が可能となった．すなわち，通信制御系の事象駆動型制御としては，対応可能な通信レベル変化の範囲が広がったことになる．また，通信路上の攻撃下での複数異常検出器の協調推定は量子化制御と離散事象システムの融合の結果得られたものであり，当初の研究成果では予定していないものである．Programmable Logic Controller のような産業用コントローラへのモデルベース型異常検出器の実装も可能となった．以上により，本研究は当初の計画以上に進展することが出来た．

(3)平成 29 年度

平成 27 年度と 28 年度の研究が当初の計画より進んだことにより，本年度では通信制御系の応用例として電力システムやマルチエージェントシステムを考慮した．特に量子化の可変化（縮退運転動作の多様化）に関して，フェールセーフ・フェールソフトに関わる研究成果を得た．

①モデルベース縮退運転システムの成果まとめ

縮退運転に関わるこれまでの基礎成果を学術論文にまとめた．モデルベース縮退運転制御に関わる基礎成果を学術論文１編（論文[6]）としてまとめた．この中で，中間者攻撃と DoS 攻撃に対する適用可能性と防御可能性について明らかにすることが出来た．また，縮退運転の状態推定方法において，制御系の制御ロジックのモデル化方法と攻撃検知範囲の関係性を明らかにし，解説記事１編（論文[2]）にまとめた．制御ロジックのモデル化方法に加えて，その安全性や特性解析をカルマン正準分解の観点から考察し，学術論文１編（論文[3]）にまとめた．

②電力システム応用

縮退運転システムを再生可能エネルギーシステムへ適用することを想定し，電力システムのフェールセーフとフェールソフトに関わる分散制御技術に着手した．

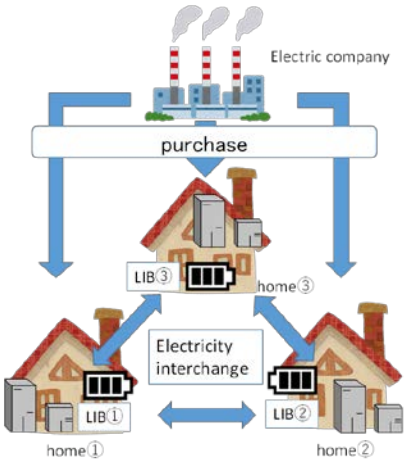

Fig. 4 自律分散エネルギーシステム

分散制御に関しては，エネファームなどのSOFC を有する家庭が複数連携することで省エネ化を実現する自律分散エネルギー運用アルゴリズム（発表[1]）を開発している（Fig.4）．アグリゲータのようにある程度の家屋数が揃わないと効力を発揮できないようなものではなく，アパートのような小規模システムを想定している．家屋連携のための家庭間共有情報をリチウムイオン蓄電池の充放電情報に置き換えることで，電力需給情報のような個人情報を利用することなく，省エネ化を実現する．

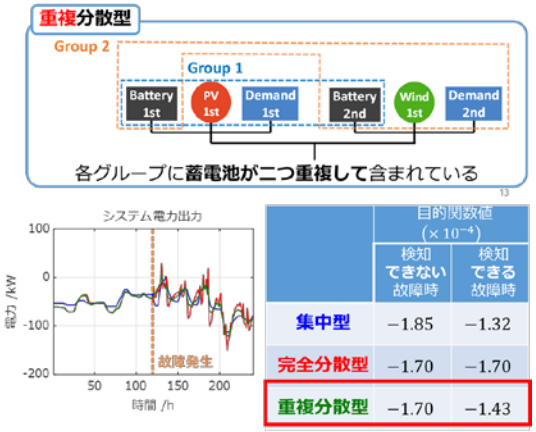

Fig. 5 グルーピング最適化

再生可能エネルギーシステムにおいて蓄電池が故障した場合，故障による性能劣化の影響を局在化する方法を１つの分散制御ユニットで管理する機器の組み合わせ（グルーピング）最適化から与えた(Fig. 5)．研究手法はモデル予測制御に基づく分散制御手法と ZDD に基づくグラフ列挙手法から構成される．前者については小規模な電力システムを対象に故障時にも継続的なシステム運用を実現する重複分散グルーピングの有効性と設計指針を明らかにした．後者については前者で得られた結果が比較的規模の大きい電力システムについても成り立つことを明らかにした．

③マルチエージェント系のフェールソフトとフェールセーフ

適用可能な通信制御系の拡大として，マルチエージェントシステムの分散協調制御のフェールセーフとフェールソフトに着手し，学術論文（論文[1]）としてまとめた．エージェント間で通信が到達できない場合，到達出来たとしてもお互いの位置を誤検知した場合，エージェントの渋滞を検出漏れした場合について，解析を行った．

④今後の展開

平成 29 年度では，縮退運転システムの適用例として複数制御システムが連携する電力システムやマルチエージェントシステムを考慮した．縮退運転動作としてのフェールセーフやフェールソフトに注目したが，サイバー攻撃が検知され要因が排除された後の安全なシステム回復手法も重要である．特に，システムが拡大化されると，サイバー攻撃が完全に除去されない中でのシステム回復技術も必要となる．

システム拡大化がサイバー攻撃状態からの回復方法を複雑化するのは事実だが，システム連携によって回復のしやすさが向上することも期待できる．そこで，システム連携を前提とした縮退運転とシステム回復を実現するレジリエントな制御システムセキュリティ手法を今後研究していく．

５．主な発表論文等

〔雑誌論文〕（計 11 件）

[1] 望月優加理，澤田賢治，新誠一，通信可能範囲を考慮した分散協調制御システムに基づく迷路探索，システム制御情報学会論文集，査読有，31 巻，2018，167-176

[2] 澤田賢治，制御システムセキュリティ技術としてのモデルベース縮退運転システム，システム/制御/情報，査読有，62 巻，2018，141-146

[3] 岸田貴光，塚田健人，澤田賢治，新誠一，組み込みシステムの無瞬断更新のためのカルマン正準分解に基づくプログラム解析，計測自動制御学会論文集，査読有，54 巻，2018，227-237，doi.org/10.9746/sicetr.54.227

[4] 澤田賢治，総論「産業システム連携のこれから－特集号発刊によせて」，計測と制御，査読有，57 巻，2018，2-3，https://doi.org/10.11499/sicejl.57.2

[5] 横川慎二，市川晴久，曽我部東馬，澤田賢治，川喜田佑介，再生可能エネルギー指向自律分散グリッドーバーチャルグリッドー，日本信頼性学会誌，査読有，39 巻，2017，8-15

[6] Tsubasa Sasaki, Kenji Sawada, Siichi shin, Shu Hosokawa, Model Based Fallback Control for Networked Control System via Switched Lyapunov Function, IEICE Transactions on Fundamentals, 査読有, E100-A, 2017, 2086-2094, 10.1587/transfun.E100.A.2086

[7] 山藤勝彦，山本建，澤田賢治，電磁比例弁内のスプールに作用するクーロン摩擦力に起因した不安定振動の解析と安定化させるための設計法，日本機械学会論文集，査読有，83 巻，2017，p.16-00553，doi.org/10.1299/transjsme.16-00553

[8] 田村健太，澤田賢治，新誠一，自動車の前後制動力配分のシミュレーションモデルベース最適化，システム制御情報学会論文集，査読有，30 巻，2017，197-208，doi.org/10.5687/iscie.30.197

[9] Hiroshi Okajima, Kenji Sawada, Nobutomo Matsunaga, Dynamic Quantizer Design under Communication Rate

Constraints, IEEE Transactions on Automatic Control, 査読有, No. 61, 2016, 3190-3196, 10.1109/TAC.2015.2509438

[10]藤田貴大, 澤田賢治, 小木曽公尚, 新誠一, RSA 公開鍵暗号を用いたネットワーク制御系のセキュリティ強化, 計測自動制御学会論文集, 査読有, 51 巻, 2015, 655-660. doi.org/10.9746/sicetr.51.655

[11]Ryosuke Nakamura, Kenji Sawada, Seiichi Shin, Kenji Kumagai and Hisato Yoneda, Model reformulation for conflict-free routing problems using Petri Net and Deterministic Finite Automaton, Journal Artificial Life and Robotics, 査読有, No.20, 262-269, 10.1007/s10015-015-0215-z

〔学会発表〕(計 41 件, うち招待講演 4 件, 国際学会 14 件)

[1] Shunsuke Kuwana, Kenji Sawada, Seiichi Shin, On autonomous distributed operation of LiB combined type SOFC system, AROB, 2018 年 1 月 23～25 日, 大分, 日本

[2] Takanori Kishida, Kenji Sawada, Seiichi Shin, On Software Update Analysis via Kalman Decomposition, ASCC, 2017 年 12 月 17 日～20 日, ゴールドコースト, オーストラリア

[3] Kenji Sawada, Model-based Cybersecurity for Control Systems: Modeling, Design and Control, SICE Annual Conference, 2017 年 9 月 19 日～22 日, 金沢, 日本

[4] Yuta Ueda, Kenji Sawada, Seiichi Shin, Control of self-organizing robots with switching role: Addition of robots in the multi columns formation moving, AROB, 2017年1月18日～20日, 大分, 日本

[5] Kenji Sawada, Quantized control based on invariant set analysis, SEMINAIRE DE L'EQUIPE MAC (LAAS-CNRS) **(招待講演)**, 2016 年 9 月 22 日, ツールーズ, フランス

[6] Kenta Tamura, Kenji Sawada, Seiichi Shin, Brake force distribution optimization using simultaneous perturbation stochastic approximation, SICE Annual Conference, 2016 年 9 月 20 日～23 日, 茨城, 日本

[7] Yukari Mochizuki, Kenji Sawada, Seiichi Shin, Multiple Agents Maze Exploration with Deadlock Avoidance, SICE Annual Conference, 2016 年 9 月 20 日～23 日, 茨城, 日本

[8] Kento Tsukada, Kenji Sawada, Seiichi Shin, A Toolchain on Model Checking SPIN via Kalman Decomposition for Control Systems Software, CASE, 2016 年 8 月 21 日～24 日, テキサス, アメリカ

[9] Kenji Sawada and Seiichi Shin, Sampled-data model following output feedback control for discrete-valued input systems, CDC, 2015 年 12 月 15 日～18 日, 大阪, 日本

[10]Kento Tsukada, Kenji Sawada, Seiichi Shin, Studies on Software Model Checking via Kalman Decomposition, CACS, 2015 年 11 月 18 日, 高雄, 台湾

[11]Kenji Sawada, Model-based Fall Back Control for Cybersecurity, 2015 Netherlands-Japan Cyber Security Conference in Tokyo **(招待講演)**, 2015 年 11 月 12 日, 東京, 日本

[12]Tsubasa Sasaki, Kenji Sawada, Seiichi Shin and Shu Hosokawa, Model Based Fallback Control for Networked Control System via Switched Lyapunov Function, IECON. 2015 年 11 月 11 日, 横浜, 日本

[13]Kenji Sawada and Seiichi Shin, Sampled-data model following control for discrete-valued input systems via improved matrix uncertainty approach, ECC, 2015 年 7 月 15 日～17 日, リンツ, オーストリア

[14]Kenji Sawada and Seiichi Shin, Reduced-order dynamic quantizer synthesis for discrete-valued input systems, ECTI-CON, 2015 年 6 月 24 日～26 日, ホアヒン, タイ

[15]Tsubasa Sasaki, Kenji Sawada, Seiichi Shin and Shu Hosokawa, A Fallback Control Study of Networked Control Systems for Cybersecurity, ASCC2015, 2015 年 5 月 31 日～6 月 3 日, コタキナバル, マレーシア

〔図書〕(計 1 件)

[1] 川田昌克, 東俊一, 市原裕之, 浦久保孝光, 大塚敏之, 甲斐健也, 國松禎明, 澤田賢治, 永原正章, 南裕樹, 倒立振子で学ぶ制御工学, 93/105, 森北出版, 2017

６．研究組織

(1)研究代表者

澤田　賢治 (SAWADA　KENJI)

電気通信大学・i-パワードエネルギー・システム研究センター・准教授

研究者番号：80550946

(2)研究分担者

該当無し

(3)連携研究者

該当無し