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

令和　２ 年　 ５ 月 ２４ 日現在

機関番号：１４５０１
研究種目：若手研究(B)
研究期間：2017～2019
課題番号：１７Ｋ１４６９９

研究課題名（和文）サイバー攻撃に対して頑強な制御システムの開発

研究課題名（英文）Design of robust control systems against cyber attacks

研究代表者
若生　将史（Masashi, Wakaiki）

神戸大学・システム情報学研究科・講師

研究者番号：５０７７８５８７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：通信ネットワークを用いた制御システムに対してサイバー攻撃が仕掛けられるシナリオを想定し，攻撃下においてもシステム全体の安全性を保証する頑強な制御器の設計理論を構築した．攻撃として観測信号の改ざんやDoS攻撃（意図的なパケットロス）を考え，また制御システムのモデルとして，微分方程式や差分方程式で記述される連続系だけでなく，オートマトンで記述される離散系も取り扱った．さらに，無線基地局の送信電力制御におけるプライバシー強化手法を開発した．

研究成果の学術的意義や社会的意義
IoT（Internet of Things）が急速に発展する現在，重要インフラなど都市に存在するあらゆるものがインターネットで繋がり，サイバー攻撃を受ける範囲が今後広がることが予想される．政府・企業の社会的信頼の失墜を未然に防ぎ，その生産性を担保しながら事業を継続するために，制御システムにおけるサイバー攻撃対策は極めて重要な課題といえる．本研究はこの課題を解決するための研究開発であり，これまで制御性能の改善を主目的としてきた制御理論にも学術的に大きなインパクトを持つものである．

研究成果の概要（英文）：We have considered networked control systems under cyber attacks and have proposed design methods of controllers that guarantee the safety of the systems. As cyber attacks, we have handled data manipulation in measurement signals as well as DoS attacks (malicious packet losses). The plant model we have considered are continuous systems described by differential equations or difference equations and also discrete systems described by automata. In addition, we have developed a privacy enhancement method for the transmission power control of wireless base stations.

研究分野：制御理論

キーワード：制御システム　セキュリティ　プライバシー　量子化制御

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

１．研究開始当初の背景

以前の制御システムは独自のプロトコルを採用し，情報システムから独立していた．しかし，生産性の向上や開発コストの削減のために，近年は汎用的なプロトコルを用いてネットワークに接続されるようになった．これらの事情により，これまでは情報システムのみを対象としていたサイバー攻撃のリスクが制御システムに範囲を広げている．制御システムがサイバー攻撃の対象になると，操業停止やライフラインの破壊など深刻な被害を受け，人命が失われる可能性さえある．また，制御システムにおいてプライバシー性の高いデータを通信する機会が増えている．例えばスマートグリッドにおいて，電力制御や電力価格調整のために，各家庭の電力消費量のデータが収集されている．もしこのような情報が盗聴されると，ライフスタイルが推測されプライバシーが侵害される懸念がある．これらの理由で，制御システムに対するセキュリティ・プライバシーの強化が緊急の課題になっていた．

２．研究の目的

制御システムの数理モデルを用いて，どのようなサイバー攻撃に対してシステムが安全に稼働するのか解析するとともに，サイバー攻撃に対して頑強な制御系の設計法を構築する．サイバー攻撃として，観測信号の改ざんや意図的にパケットロスを起こす DoS 攻撃に焦点を当てる．また制御システムのモデルとして，微分方程式や差分方程式で記述される連続系だけでなく，オートマトンで記述される離散系も取り扱う．

さらに，制御システムにおけるプライバシーの強化に取り組む．プライバシーを強化することで，制御システムが冗長化し，制御性能が悪化する可能性がある．そこで，プライバシーレベルと制御性能の間のトレードオフを解明し，性能悪化を抑えながらプライバシー強化を実現するアルゴリズムを開発する．

３．研究の方法

セキュリティとプライバシーの観点から，制御システムのサイバー攻撃に対する頑強性を保証することを目指して，以下の課題に取り組む．

(1) 観測信号の改ざんに対して頑強な制御

観測信号がすべて改ざんされた場合，フィードバック制御が全く機能しなくなることは言うまでもない．しかし，観測信号の一部のみが改ざんされた場合は，フィードバック制御が機能しうると予想できる．ここで生じる数理的な課題として，どの程度多くの観測信号が改ざんされると制御不能になるのか，そしてそれは制御系のどのような性質と関連して決まるのか，というものがある．制御対象が連続系や離散系である場合に関して，サイバー攻撃に対する頑強性の解析を行うとともに，サイバー攻撃に対してシステムが「強く」なる制御器の設計問題に取り組む．

(2) DoS 攻撃下のおけるネットワーク化制御

観測信号のパケット通信を妨害する DoS 攻撃の下で，ネットワーク化制御システムが安全に稼働するための制御系設計問題を考える．パケットロスが起こる頻度が高ければ高いほど，システムを安定化するためには大きな通信量が必要になるはずである．本研究では，パケットロスが起こる頻度と安定化のための通信量の間のトレードオフを解明する．そして，制御対象とパケットロスの頻度が与えられたときに，システムが安定となる量子化則が存在するための条件を求め，そのような量子化則の設計法を構築する．

(3) プライバシーを考慮した無線基地局の送信電力制御

送信電力を決定する制御器と無線基地局の間の通信路においてデータが盗聴されうる状況を考える．まず，所望のプライバシーレベルを達成するために，従来の手法でどの程度制御性能が低下してしまうのか検証する．次に，制御性能を維持したまま，高いプライバシーレベルを保証するための送信電力の制御手法を考える．さらに，差分プライバシーを指標として，プライバシーレベルと制御性能の関係性を調べる．

４．研究成果

本研究で得られた成果のうち主たるものを以下にまとめる．

(1) 観測信号の改ざんを許容する制御アルゴリズムの構築

連続系に対して，観測信号の一部が改ざんされてもシステム全体が正常に機能するための制御アルゴリズムを構築した．このアルゴリズムは２つの大きな特徴を有している．１つ目は，従来手法ではオブザーバの群を構築して，改ざんされた観測信号を特定していたが，提案手法ではオブザーバの群の代わりに，状態空間の次元が大きなオブザーバを用いている点である．これによって，リアルタイム計算に必要なメモリを大きく削減することができた．２つ目は出力改ざんの検出を充足可能性問題（SMT）に帰着させた点である．その結果，SMT ソルバを利用して低い計算量で迅速に攻撃検出が可能となった．

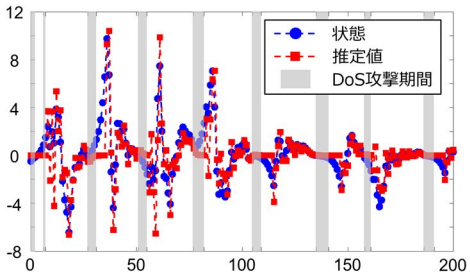
また，離散系に関して，コンピュータシステムに対するマルチレイヤーのサイバー攻撃を

オートマトンで表現した．そして，攻撃下においても所望の仕様を達成するスーパバイザが存在するための条件を，制御対象の可観測性によって特徴づけるとともに，攻撃に対して頑強なスーパバイザの設計法を考案した．従来手法を用いると，仕様を満たすスーパーバイザの設計法における計算量は，サイバー攻撃の種類数に関して指数的に増加してしまうが，提案手法では計算量をサイバー攻撃の種類数の２乗に抑えることができるという利点がある．

(2) DoS 攻撃を考慮した量子化則の設計

パケットロスを考慮した従来研究の多くは，パケットロスに対して確率的なモデルを用いていた．しかし，DoS 攻撃に対してそのような確率的なモデルを使うことはできない．これは，パケットロスを起こすかどうかを攻撃者が自由に決めることができるためである．そこで本研究では，確定的な条件によってパケットロスが起こる長さと頻度を記述した．そして，量子化則の１種である，ズーミングイン，ズーミングアウト機構を DoS 攻撃下でも正常に機能するように拡張した．そして，システム全体がリアプノフ安定であり，さらに状態が原点に収束するための十分条件を，パケットロスが起こる長さ・頻度と通信量を用いて記述し，これらの間のトレードオフに対する部分的な結果を得た．

図１と２は，回分式反応器の数理モデルに対して，提案した量子化則を適用して得られた時間応答である．安定性に関する十分条件を満たす場合の時間応答が図１であり，そうでない場合の時間応答が図２である．このモデルの状態空間の次元は４であり，図１と２の青丸は状態の１つをプロットしたものである．また，その推定値を赤四角でプロットしている．灰色で覆われた期間は，DoS 攻撃によって観測信号のパケットが欠落している期間を表している．十分条件が満たされている図１は，状態と推定値がどちらも原点に収束しているが，十分条件が満たされていない図２では，原点の収束が達成されておらず安定化できてないことが確認できる．



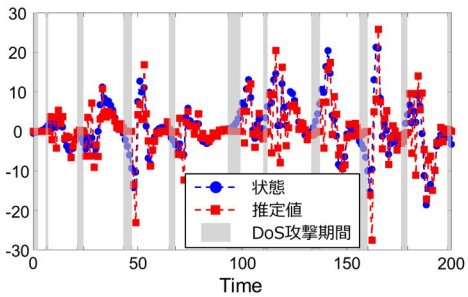


図１：十分条件を満たす場合の時間応答　図２：十分条件を満たさない場合の時間応答

(3) 秘匿性を有する分散型アルゴリズムの開発

太陽光発電などの環境発電とバッテリーを用いてオフグリッドで稼働するスモールセル無線基地局（図３）を対象として，ユーザ位置を秘匿しながら送信電力を決定するアルゴリズムを考案した．環境発電は一般に予測が困難であり，バッテリーの充電率は不安定になりやすい．そのため，無線基地局が収容するユーザ数とバッテリーの充電率を考慮しつつ無線基地局の送信電力を制御する必要がある．従来の制御方式では，点在する無線基地局からユーザ数に関するデータを集約し，大域的な最適化問題を解くことで送信電力を決定していた．ユーザ数を秘匿化するためには意図的にノイズを印加すればよいが，ノイズによって制御性能が悪化してしまう．そこで本研究では，分散最適化の手法を適用することで，制御性能の劣化を抑えながら所望のプライバシーレベルを保証するアルゴリズムを構築した．また，提案した分散的アルゴリズムに関して，差分プライバシーを指標として用いて，プライバシーレベルと制御性能との間のトレードオフを解析した．

図３：スモールセル基地局

(4) ネットワーク化制御系の安定性解析

少ない通信回数でシステムを安定化することを目的として，必要なときだけ出力の測定や制御入力の更新を行うイベント駆動制御や自己駆動制御について新たな手法を提案した．イベント駆動制御では，制御対象に備えられたセンサが，観測信号を送信するか決定する．一方，自己駆動制御では，制御器がリアルタイムで観測信号の送信時刻を計算し，それをセンサに伝達する．制御対象として無限次元系を考え，強連続半群論に基づいて，イベント駆動則や自己駆動則を組み込んだ制御システムが指数安定となるための十分条件を導出した．また，時間遅れを含む系や熱拡散系など様々なシステムに対して提案法が適用可能であることを示した．この過程で，周期的に出力の測定や制御入力の更新を行う従来のサンプル値制御システムにおいても，ロバスト安定性解析に関する新たな知見を得ることができた．

５．主な発表論文等

〔雑誌論文〕　計17件（うち査読付論文　17件／うち国際共著　6件／うちオープンアクセス　0件）

１．著者名 Wakaiki Masashi, Yamamoto Yutaka	４．巻 -
２．論文標題 Stability analysis of perturbed infinite-dimensional sampled-data systems	５．発行年 2020年
３．雑誌名 Systems & Control Letters	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.sysconle.2020.104652	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Wakaiki Masashi, Cetinkaya Ahmet, Ishii Hideaki	４．巻 -
２．論文標題 Stabilization of networked control systems under DoS attacks and output quantization	５．発行年 2020年
３．雑誌名 IEEE Transactions on Automatic Control	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2019.2949096	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Wakaiki Masashi, Sano Hideki	４．巻 32
２．論文標題 Sampled-data output regulation of unstable well-posed infinite-dimensional systems with constant reference and disturbance signals	５．発行年 2020年
３．雑誌名 Mathematics of Control, Signals, and Systems	６．最初と最後の頁 43--100
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/s00498-019-00252-9	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Wakaiki Masashi	４．巻 65
２．論文標題 An LMI approach to stability analysis of coupled parabolic systems	５．発行年 2020年
３．雑誌名 IEEE Transactions on Automatic Control	６．最初と最後の頁 404--411
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2019.2916534	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名	4．巻
Koiwa Kenta, Kuribayashi Toru, Zanma Tadanao, Liu Kang-Zhi, Wakaiki Masashi	13
2．論文標題	5．発行年
Optimal current control for PMSM considering inverter output voltage limit: model predictive control and pulse-width modulation	2019年
3．雑誌名	6．最初と最後の頁
IET Electric Power Applications	2044--2051
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1049/iet-epa.2019.0225	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Wakaiki Masashi, Zanma Tadanao, Liu Kang-Zhi	64
2．論文標題	5．発行年
Observer-based stabilization of systems with quantized inputs and outputs	2019年
3．雑誌名	6．最初と最後の頁
IEEE Transactions on Automatic Control	2929--2936
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1109/TAC.2018.2873355	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Wakaiki Masashi, Suto Katsuya, Koiwa Kenta, Liu Kang-Zhi, Zanma Tadanao	3
2．論文標題	5．発行年
A control-theoretic approach for cell zooming of energy harvesting small cell networks	2019年
3．雑誌名	6．最初と最後の頁
IEEE Transactions on Green Communications and Networking	329--342
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1109/TGCN.2018.2889897	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	－

1．著者名	4．巻
Wakaiki Masashi, Tabuada Paulo, Hespanha Joao P.	9
2．論文標題	5．発行年
Supervisory control of discrete-event systems under attacks	2019年
3．雑誌名	6．最初と最後の頁
Dynamic Games and Applications	965--983
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
https://doi.org/10.1007/s13235-018-0285-3	有
オープンアクセス	国際共著
オープンアクセスではない、又はオープンアクセスが困難	該当する

1．著者名 Okano Kunihisa, Wakaiki Masashi, Yang Guosong, Hespanha Joao P.	4．巻 63
2．論文標題 Stabilization of networked control systems under clock offsets and quantization	5．発行年 2018年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 1708--1723
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2017.2753938	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Wakaiki Masashi, Ogura Masaki, Hespanha Joao P.	4．巻 56
2．論文標題 LQ-optimal sampled-data control under stochastic delays: Gridding approach for stabilizability and detectability	5．発行年 2018年
3．雑誌名 SIAM Journal on Control and Optimization	6．最初と最後の頁 2634--2661
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1137/17M1150608	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Wakaiki Masashi	4．巻 2
2．論文標題 Stability analysis and l2-gain of adaptive control systems with event-triggered try-once-discard protocols	5．発行年 2018年
3．雑誌名 IEEE Control Systems Letters	6．最初と最後の頁 157--162
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LCSYS.2017.2777739	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shoukry Yasser, Chong Michelle, Wakaiki Masashi, Nuzzo Pierluigi, Sangiovanni-Vincentelli Alberto, Seshia Sanjit A., Hespanha Joao P., Tabuada Paulo	4．巻 2
2．論文標題 SMT-based observer design for cyber-physical systems under sensor attacks	5．発行年 2018年
3．雑誌名 ACM Transactions on Cyber-Physical Systems	6．最初と最後の頁 1--27
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3078621	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Wakaiki Masashi, Yamamoto Yutaka	4．巻 11
2．論文標題 Stabilisation of switched systems with sampled and quantised output feedback	5．発行年 2017年
3．雑誌名 IET Control Theory & Applications	6．最初と最後の頁 1913--1921
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/iet-cta.2016.1299	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Wakaiki Masashi, Okano Kunihisa, Hespanha Joao P.	4．巻 81
2．論文標題 Stabilization of systems with asynchronous sensors and controllers	5．発行年 2017年
3．雑誌名 Automatica	6．最初と最後の頁 314--321
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.automatica.2017.04.005	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Wakaiki Masashi and Yamamoto Yamamoto	4．巻 62
2．論文標題 Stabilization of switched linear systems with quantized output and switching delays	5．発行年 2017年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 2958--2964
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2016.2604924	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ogura Masaki, Wakaiki Masashi, Rubin Harvey, and Preciado Victor M.	4．巻 95
2．論文標題 Delayed bet-hedging resilience strategies under environmental fluctuations	5．発行年 2017年
3．雑誌名 Physical Review E	6．最初と最後の頁 1--8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevE.95.052404	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 小岩 健太，鈴木 賢太，劉 康志，残間 忠直，若生 将史，田村 淳二	４．巻 137
２．論文標題 H∞制御による電力貯蔵装置の容量低減化	５．発行年 2017年
３．雑誌名 電気学会論文誌Ｂ（電力・エネルギー部門誌）	６．最初と最後の頁 596--597
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejpes.137.596	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　11件）

１．発表者名 若生 将史，佐野 英樹
２．発表標題 無限次元系のイベント駆動制御について
３．学会等名 2019年度応用数学合同研究集会
４．発表年 2019年

１．発表者名 Wakaiki Masashi, Suto Katsuya, Masubuchi Izumi
２．発表標題 Privacy preserved cell zooming with distributed optimization in green networks
３．学会等名 90th IEEE Vehicular Technology Conference（国際学会）
４．発表年 2019年

１．発表者名 Sano Hideki, Wakaiki Masashi, Maruyama Hayate
２．発表標題 Backstepping observers for two linearized Kermack-McKendrick models
３．学会等名 17th IFAC Workshop on Control Applications of Optimization（国際学会）
４．発表年 2018年

１．発表者名
Iimura Yoshinobu, Wakaiki Masashi, Homma Katsumi, Umeda Yuhei, Kaneko Junji, Higuchi Hiroyuki, Kubota Kazumi, Asami Naoya, Ikeda Kazuto

２．発表標題
Simultaneous optimization of statistical model and control input plan

３．学会等名
2018 Annual American Control Conference（国際学会）

４．発表年
2018年

１．発表者名
Wakaiki Masashi, Cetinkaya Ahmet, Ishii Hideaki

２．発表標題
Quantized output feedback stabilization under DoS attacks

３．学会等名
2018 Annual American Control Conference（国際学会）

４．発表年
2018年

１．発表者名
Wakaiki Masashi, Suto Katsuya, Koiwa Kenta, Liu Kang-Zhi, Zanma Tadanao

２．発表標題
Model predictive cell zooming for energy-harvesting small cell networks

３．学会等名
2018 IEEE International Conference on Communications（国際学会）

４．発表年
2018年

１．発表者名
若生 将史, Ahmet Cetinkaya, 石井 秀明

２．発表標題
DoS攻撃の下での量子化制御

３．学会等名
第61回システム制御情報学会研究発表講演会

４．発表年
2018年

１．発表者名
若生 将史, 佐野 英樹

２．発表標題
無限次元システムのサンプル値サーボ問題について

３．学会等名
2018年度応用数学合同研究集会

４．発表年
2018年

１．発表者名
Li Guang-Bo, Zanma Tadanao, Wakaiki Masashi, Liu Kang-Zhi

２．発表標題
Design of networked control systems in consideration of quantization error and channel capacity

３．学会等名
36th Chinese Control Conference（国際学会）

４．発表年
2017年

１．発表者名
Takagi Yu, Koiwa Kenta, Zanma Tanadano, Wakaiki Masashi, Liu Kang-Zhi

２．発表標題
Electrical angle estimation of rotor for PMSM in model predictive current control

３．学会等名
36th Chinese Control Conference（国際学会）

４．発表年
2017年

１．発表者名
Takayasu Syuntaro, Zanma Tadanao, Wakaiki Masashi, Liu Kang-Zhi

２．発表標題
Stability and performance analysis of receding horizon quantizer in single-input system

３．学会等名
36th Chinese Control Conference（国際学会）

４．発表年
2017年

１．発表者名
Hashimoto Daiki, Zanma Tadanao, Wakaiki Masashi, Liu Kang-Zhi

２．発表標題
Estimation of network traffic status for networked control systems with data dropout and its control

３．学会等名
36th Chinese Control Conference（国際学会）

４．発表年
2017年

１．発表者名
Wakaiki Masashi, Zanma Tadanao, Liu Kang-Zhi

２．発表標題
Quantized output feedback stabilization by Luenberger observers

３．学会等名
20th IFAC World Congress（国際学会）

４．発表年
2017年

１．発表者名
Wakaiki Masashi, Ogura Masaki, Hespanha Joao P.

２．発表標題
Linear quadratic control for sampled-data systems with stochastic delays

３．学会等名
2017 Annual American Control Conference（国際学会）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考