三菱電機技報　99巻8号(通巻1122号)　ISSN 0369-2302/CODEN:MTDNAF

MITSUBISHI ELECTRIC
Changes for the Better

三菱電機技報

8
2025
Vol.99 No.8

持続的な事業成長を牽引するデジタル技術(前編)

No.8

特　集　持続的な事業成長を牽引するデジタル技術(前編)　Digital Technologies for Sustainable Business Growth (The first part)

巻頭言

三菱電機では，サステナビリティ経営を実現するビジネスエリアとして，「インフラ」「インダストリー・モビリティ」「ライフ」を設定しています。

三菱電機技報ではこのビジネスエリアを中心に特集を紹介しています。

今回の特集では全エリアを支える基盤となる“持続的な事業成長を牽引するデジタル技術(前編)”をご紹介します。

巻頭言

持続的な事業成長を牽引するデジタル技術

Digital Technologies for Sustainable Business Growth

岡　　徹　*Toru Oka*

上席執行役員 知的財産担当 研究開発本部長（博士（工学））

Executive Officer, In charge of Intellectual Property, Vice President, Corporate Research and Development

三菱電機グループは，サステナビリティの実現を経営の根幹に位置付けて，社会・環境貢献と更なる事業発展を目指して，リスクを恐れず新たな発想で価値を創出する“イノベーティブカンパニー”へと変革します。強みであるコンポーネント技術とデジタル技術を活用し，基盤技術を深化させることで，持続的な事業成長を牽引（けんいん）する研究開発を推進します。さらに，社会や事業に大きなインパクトを与えるフォアサイトテクノロジーの開発に注力し，社会課題の根本的な解決と革新的なアイデアによる新たな価値創出に挑戦します。

イノベーティブカンパニーへの変革で，デジタル技術は鍵になる重要な技術です。新たな価値やソリューションに転換するためのデジタル技術を，デジタル基盤“Serendie”（セレンディ）を活用して得られるデータを基に，更に強化することで，製品やシステムの効率性や安全性を向上させるだけでなく，新しいビジネスモデルの創出やサービスの提供も可能にします（**図1**）。

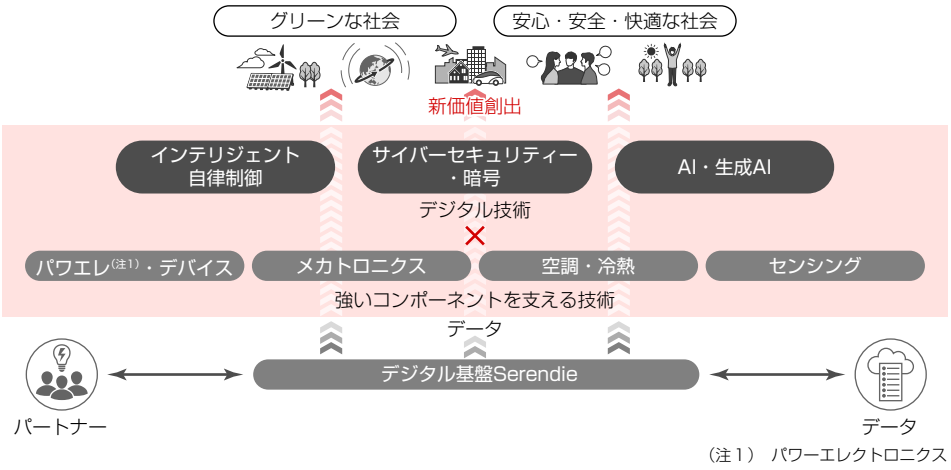


図1－強化する技術領域

三菱電機技報８月号では，“インテリジェント自律制御技術”と“サイバーセキュリティー・暗号技術”に関する具体例を，９月号では“AI・生成AI技術”と“フォアサイトテクノロジー”に関する具体例を紹介します。

“インテリジェント自律制御技術”ではFA・ビル・空調機器・宇宙などで培った様々な制御関連技術を強みとして，多くのコンポーネントやシステムが複雑に連携する大規模なシステムに対して，統合的な運用・管理と自律的な稼働を実現し，ビル・データセンター・工場・地域まで，多様なシーンでグリーンと安心・安全・快適を実現していきます。

サイバー攻撃の手口や技術はますます巧妙化しており，大きな社会課題の一つです。エネルギーやファシリティなどの重要インフラで培った“サイバーセキュリティー・暗号技術”は，攻撃を受けた際の影響を最小化します。また，攻撃検知技術，秘匿検索技術，耐量子計算機暗号技術に注力し，サイバー攻撃に対する防御能力を高めていきます。

“AI・生成AI技術”では，コンポーネント技術で培った物理モデル，シミュレーション，そして当社AIブランド“Maisart”（マイサート）として多くの製品に搭載されたコンパクトなAIを強みとして，製造現場や保守などの変化の激しい環境に対応する，適応性と信頼性が高いAIを提供します。これによって，現場特有のデータが少量であっても高速・

高精度に推論と自動化を実現し，複雑な操作や作業を柔軟にサポートすることでユーザーの負荷軽減と効率化を実現します。今後は，物理モデルやドメイン知識を活用して高精度に予測・制御するための“Neuro-Physical AI”，安心・安全にAIを活用するための“セキュアAI”，複数のAIを最適に制御して人と協調する“エージェントAI”の三つの基盤技術に注力し，当社の特長を生かしたAIで電力システム，空調システム，交通システム，防衛システムなどの幅広い事業領域で新たな価値を提供していきます。

“フォアサイトテクノロジー”とは，将来の社会や事業に大きなインパクトを与えることを目指して，先見の明を持って開発する技術です。革新的な新技術や既存技術の組合せで社会や事業に大きなインパクトを与えて，社会課題解決に貢献するため，技術ポテンシャルや社会的価値などを分析してテーマを抽出し，新たな価値創出に挑戦していきます。光電融合技術やカーボンリサイクル技術，量子関連技術などのエネルギー問題や環境問題の解決に大きく貢献する可能性を秘めた技術開発を，具体的な事業仮説を描いて，将来の事業成長を牽引する技術として投資を行っていきます。

私たち三菱電機グループは，“イノベーティブカンパニー”へと変革し，持続的な事業成長を牽引するデジタル技術や革新技術の研究開発を推進し，多様化・深刻化する社会課題の解決に取り組むことで持続可能な社会の実現に貢献していきます。

特集論文

高周波半導体デバイスの自律的バイアス制御技術

山口裕太郎*
Yutaro Yamaguchi

*情報技術総合研究所(博士(工学))

Autonomous Bias Control Technology for High－Frequency Semiconductor Devices

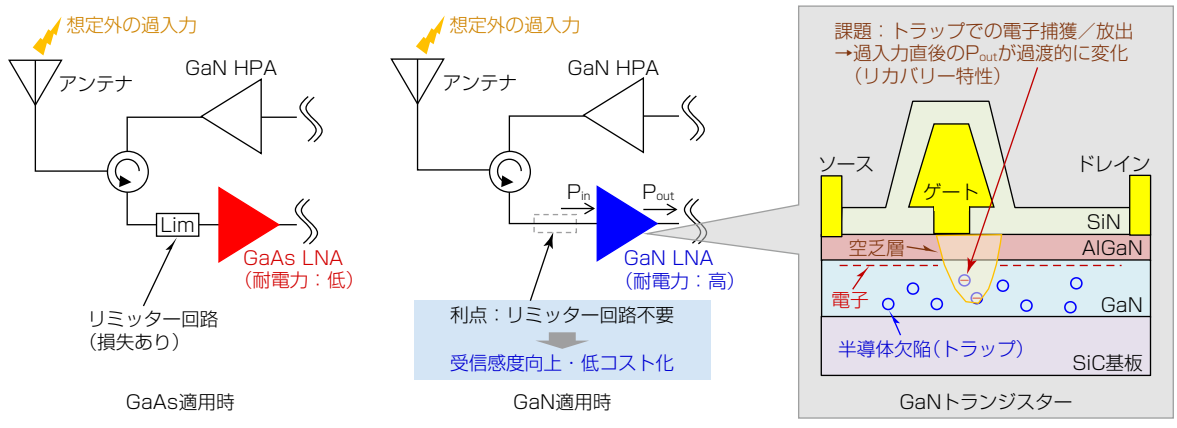
要　旨

レーダー・通信システムへの適用が検討されている高耐電力なGallium Nitride(GaN：窒化ガリウム)低雑音増幅器(Low Noise Amplifier：LNA)は半導体欠陥(トラップ)の影響で過入力直後のロバストな動作の実現が難しかった。これを解決するために，トランジスター自身のトラップを利用してバイアス電圧を自律的に変化させることによって，出力電力の過渡的な変化ΔP_{out}を抑制し，ロバストな動作を可能にする回路を開発した。この回路を試作・検証した結果，室温(300K)でΔP_{out}を2.4dBから0.2dBに低減し，高温(350K)でも1.9dBから0.2dBに低減し，この回路の有効性を確認した。

1. ま え が き

レーダー・通信システムの高周波モジュールで送信側の高出力増幅器(High Power Amplifier：HPA)にGaNを適用するだけでなく，受信側のLNAにもGaNを適用することが検討されている。**図1**に，LNAにGaNを適用したときの利点と課題を示す。GaN適用の利点は従来のGallium Arsenide(GaAs：ガリウムヒ素)よりも高耐電力なGaNに置き換えることで想定外の過入力からLNAを保護するためのリミッター回路が不要になることである。これによってGaAsに比べてGaNは高周波モジュール全体としての受信感度向上及び低コスト化を実現できる。一方，置き換えに向けたGaN LNAの技術的な課題の一つがリカバリー特性の改善である。リカバリー特性はLNAへの想定外の過入力の直後にGaNトランジスター内のトラップの影響で出力電力P_{out}がμsからmsのオーダーで過渡的に変化する。これはGaN特有の課題であり，ロバストな動作を阻害する要因になっている。

本稿ではGaN LNAのリカバリー特性の改善のために独自に開発した自律的バイアス制御回路について概要を述べる。詳細については参考文献(1)を参照されたい。



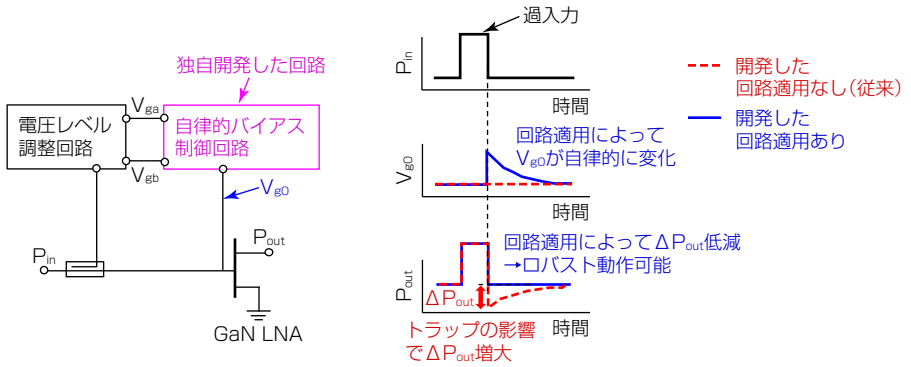
SiN：窒化ケイ素，AlGaN：窒化アルミニウムガリウム，SiC：シリコンカーバイド

図1 －NAにGaNを適用したときの利点と課題

2. 自律的バイアス制御回路

図2に，開発した自律的バイアス制御回路のコンセプトを示す。**図2**(a)に回路構成を示しており，開発した自律的バイアス制御回路はLNAのゲートバイアス電圧V_{g0}を自律的に変化させる。入力電力P_{in}のレベルに応じて電圧レベル調整回

路でV_{ga}及びV_{gb}を出力し，それらの電圧がこの回路に入力される。そして，この回路ではP_{in}に基づくV_{ga}及びV_{gb}の変化に応じて過入力直後のV_{g0}のレベルを変化させる。**図2**(b)にP_{in}，V_{g0}，P_{out}のタイムチャートを示す。この回路を適用しない場合，LNAのゲートバイアス電圧V_{g0}は一定である。その場合，過入力直後トラップの影響でLNAの出力電力P_{out}が一時的に低下し過渡的に回復するリカバリー特性を示す。すなわち，この回路適用なしの場合，ΔP_{out}が大きい。一方，この回路を適用した場合，過入力直後のV_{g0}は定常状態よりも高くなり，時間経過で定常状態に戻る。また，その時定数はこの回路を適用しない場合に生じるP_{out}の過渡的変化の時定数と同程度になる。このようにV_{g0}の自律的な変化によってトラップの影響を補償して過入力直後のΔP_{out}を低減し，リカバリー特性を改善することが可能になる。



(a)　回路構成　　(b)　P_{in}，V_{g0}，P_{out}のタイムチャート

図2－自律的バイアス制御回路のコンセプト[1]

図3に自律的バイアス制御回路の回路図を示す。LNA内の補償対象になるトランジスター(Tr)はTr0とする。自律的バイアス制御回路は主にスイッチング用トランジスターTr1，ストレス印加用トランジスターTr2，抵抗R_0，R_1，R_2，R_3で構成されている。**図3**に示すように，それらのトランジスターは同じGaNチップ上に製造されるため，それぞれのTrは同じ特性のトラップを持つ。この回路では，V_{ga}及びV_{gb}が過入力時にストレスバイアスとしてTr2のドレイン及びゲートに印加され，過入力後にTr2のオン抵抗がトラップの影響によって過渡的に変化する。このTr2のオン抵抗の変化を利用して，過渡的に変化する電圧V_{g0}を生成できる。Tr2はTr0自身と同じ特性のトラップを持つため，V_{g0}の時定数は，この回路を適用しないときのP_{out}の時定数とほぼ同じになる。そのため，この回路はV_{g0}の適切なバイアス変化を自律的に生み出すことが可能になり，トラップの影響を補償してリカバリー特性を改善できる。さらに環境温度T_{amb}が変化したときトラップの物理的な特性の変化によって時定数が変化するが，この回路ではTr0内のトラップと同様にTr2内のトラップも物理的に変化するため，環境温度の変化にも自律的に対応することが可能である。Tr1はスイッチとして用いられ，V_{gb}をTr1のゲートに印加することで，必要なタイミングで所望のV_{g0}を得ることができる。抵抗R_0，R_1，R_2，R_3はTr0，Tr1，Tr2に所望の電圧が印加されるように設計されるパラメーターである。

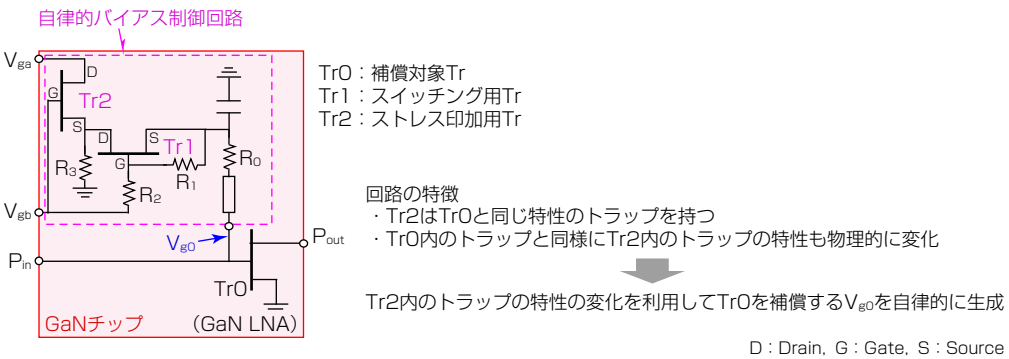


図3－自律的バイアス制御回路の回路図[1]

3. 回 路 設 計

自律的バイアス制御回路を設計し，シミュレーションでその効果を検証した。回路設計でTr0，Tr1，Tr2に所望の電圧が印加されるように抵抗R_0，R_1，R_2，R_3を設計した。**図４**に，設計した回路のリカバリー特性及びV_{g0}のシミュレーション結果を示す。シミュレーションにはトラップの影響を考慮した大信号モデルを用いた[2]。周波数は28GHz，ドレイン電圧V_dは24V，アイドルドレイン電流I_{dq}は50mA/mm，過入力時間t_Hは100μsである。過入力時のP_{in}は25dBmであり，定常時のP_{in}は３dBmである。過入力時の(V_{ga}，V_{gb})は(13.3V，－8.9V)に設定し，定常時の(V_{ga}，V_{gb})は(－5.7V，－1.95V)に設定した。**図４**(a)に示すように，自律的バイアス制御回路なしのときのV_{g0}は一定であるが，回路ありのときは過入力直後のV_{g0}は定常状態よりも高く，時間経過で定常状態に戻ることを確認した。また，**図４**(b)(c)に示すように，この回路を適用することでΔP_{out}が低減し，リカバリー特性が改善することを確認した。

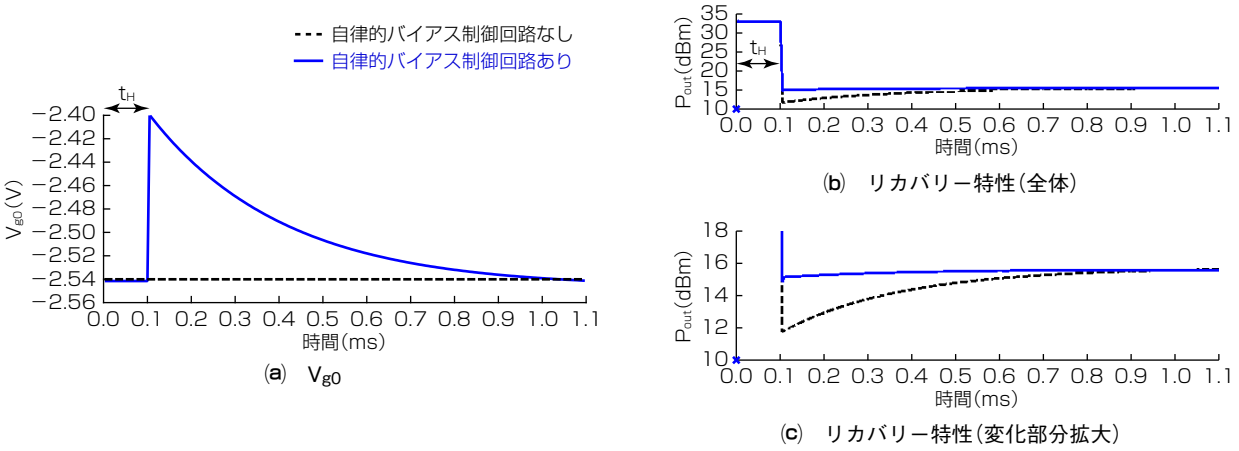


図４−設計した回路のリカバリー特性及びV_{g0}のシミュレーション結果[1]

4. 試作・検証

自律的バイアス制御回路を試作し，その有効性について原理検証を行った。**図５**に試作したGaNチップの写真を示す。チップ内のトランジスター(Tr0，Tr1，Tr2)は三菱電機製のゲート長0.19μmのGaN High Electron Mobility Transistorである。基板は50μm厚のSiCである。このチップはリカバリー特性を測定するためのTest Elementary Groupであり，Tr0の入力と出力に利得整合のプリマッチ回路を接続している。整合回路には薄膜抵抗，エピ抵抗，及び金属絶縁体金属コンデンサーを使用している。**図５**に示すように，Tr1とTr2を含む自律的バイアス制御回路は，Tr0と同じチップ上に製造され，Tr0のゲートに接続されている。P_{in}のレベルに基づいて変化するV_{ga}とV_{gb}が自律的バイアス制御回路に入力される。Tr0のゲート幅は８フィンガー×52μmであり，自律的バイアス制御回路内のTr1とTr2のゲート幅は１フィンガー×52μmである。

図６にリカバリー特性及びV_{g0}の測定結果を示す。周波数は28GHz，V_dは24V，I_{dq}は50mA/mm，過入力時間t_Hは150μsである。過入力時のP_{in}は25dBmであり，定常時のP_{in}は３dBmである。**図６**(a)(b)に示すように，T_{amb}＝300Kで自律的バイアス制御回路なしのΔP_{out}は2.4dB程度であるが，回路ありのΔP_{out}は0.2dB程度まで低減していることを確認した。また，**図６**(c)で示すように，自律的バイアス制御回路なしのときのV_{g0}は常に一定であるが，回路ありのとき，過入力直後のV_{g0}は定常状態よりも高く，時間経過で定常状態に戻ることを確認した。その時定数はP_{out}の時定数とほぼ同じである。その結果，入力電力に応じたV_{g0}の自律的な変化によってTr0のトラップの影響を適切に補償し，リカバリー特性を改善することを確認した。また，T_{amb}＝350Kでも自律的バイアス制御回路なしのΔP_{out}は1.9dB程度であるが，回路ありのΔP_{out}は0.2dB程度まで低減していることを確認した(**図６**(d)(e))。高温になると，トラップの電子を放出する時定数が短くなるため，回路なしのときのP_{out}の時定数は，T_{amb}＝300Kのときよりも短くなるが，回路適用時のV_{g0}の時定数も同様に高温で短くなる(**図６**(f))。そのため，高温時でもこの回路はトラップの影響を適切に補償できる。環境温度が

変化したときでも，環境温度に応じたV_{g0}の自律的な変化によってリカバリー特性が改善することを確認した。これらの結果から，この回路は原理的に有効であることを確認した。

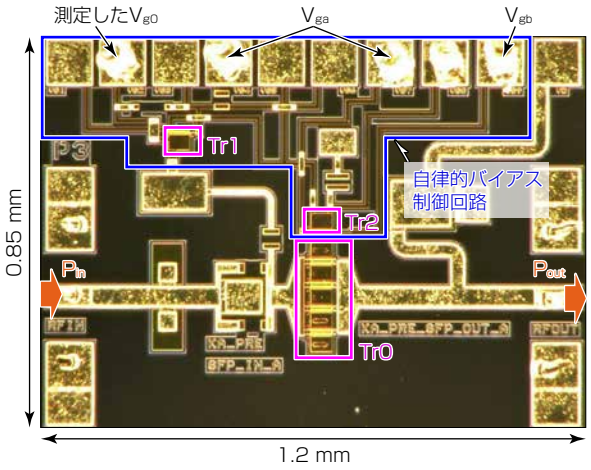
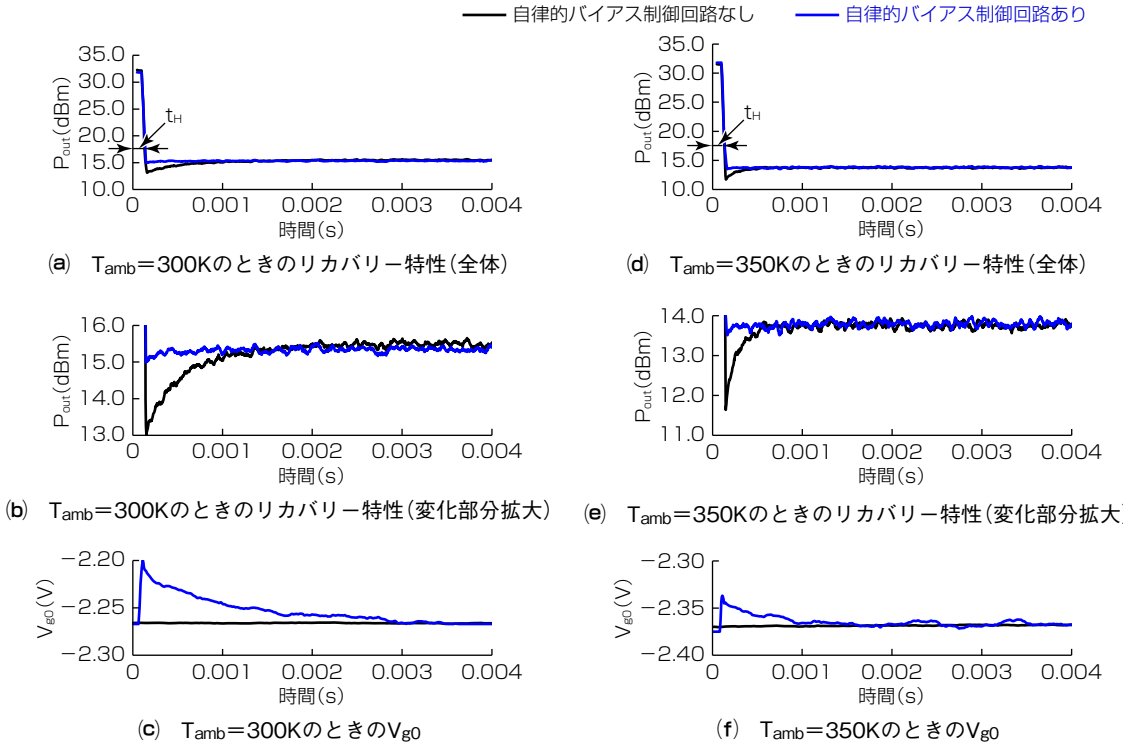


図５−試作したGaNチップ(1)



(a)　Tamb＝300Kのときのリカバリー特性(全体)

(d)　Tamb＝350Kのときのリカバリー特性(全体)

(b)　Tamb＝300Kのときのリカバリー特性(変化部分拡大)

(e)　Tamb＝350Kのときのリカバリー特性(変化部分拡大)

(c)　Tamb＝300KのときのVg0

(f)　Tamb＝350KのときのVg0

図６−リカバリー特性及びV_{g0}の測定結果(1)

5. む　す　び

GaN LNAのリカバリー特性の改善に向けて独自に開発した自律的バイアス制御回路について述べた。この回路は入力電力や環境温度が変化してもトラップの影響を自律的に補償し，ロバストな動作を実現できることを確認した。また，この回路はLNAと同じGaNチップ上に構成されるため，従来必要とされたリミッター回路に比べてコスト面でも有利であり，GaAs LNAに対するGaN LNAの優位性を維持できる。

今後はこの回路のレーダー用高周波モジュールへの実装を検討する。また，この回路を5G(第５世代移動通信システム)基地局GaNモジュールへ応用展開し，トラップが要因で劣化する歪(ひずみ)特性の改善を検討する。

参 考 文 献

(1) Yamaguchi, Y. et. al.：Trapping Compensation for Transient Recovery in GaN LNAs, IEEE Transactions on Microwave Theory and Techniques, **72**, No.7, 4006～4016 (2024)
(2) Yamaguchi, Y. et. al.：Ka-Band GaN Large-Signal Model Considering Trap Effect on Nonlinear Capacitance by Using Transient S-Parameters Measurement, IEEE BiCMOS and Compound Semiconductor Integrated Circuits and Technology Symposium (2018)

特集論文

パワー半導体の高効率駆動を実現する最新のデジタルゲート駆動技術

Cutting－Edge Digital Gate Drive Technology for High－Efficiency Power Semiconductor Operation

諸熊健一* *Kenichi Morokuma*
高宮　真† *Makoto Takamiya*
和田幸彦* *Yukihiko Wada*
山岡祐太* *Yuta Yamaoka*

*三菱電機㈱ 先端技術総合研究所
†東京大学

要　旨

2050年のカーボンニュートラルの実現に向けて，再生可能エネルギーの利用等，パワーエレクトロニクス機器(以下“パワエレ機器”という。)の存在感が増している。現在のパワエレ機器は，パワーデバイスのスイッチング動作を活用した電力変換技術が基盤になる。スイッチング動作で発生する電力損失と電磁ノイズには相反関係があり，この相反関係を改善するデジタルゲート駆動技術が注目されている。

今回，汎用のゲートドライバーICを使って，駆動信号強度を最適なタイミングで３回変化させる駆動方法を東京大学との共同研究で提案した。従来の駆動方式と比較して50Aで25%，100Aで18%のスイッチング損失(ターンオン時)を低減できて，パワエレ機器の更なる省エネルギーへの貢献が期待できる結果になった。

1. ま え が き

パワーデバイスはゲート駆動信号に応じてスイッチング動作をするが，そのスイッチング動作中に駆動信号強度を複数回離散的に変化させるデジタルゲート駆動技術が注目されている。デジタルゲート駆動技術はパワーモジュールのスイッチング損失と電磁ノイズの相反関係を改善する技術であり，駆動信号強度を変化させるタイミングを負荷電流I_Lや温度等の動作条件に応じて変更できる[(1)]。例えば駆動信号の強度を３回変化させる場合，**図１**に示すように駆動信号の強度を変化させるタイミングt_1とt_2は，パワーモジュールのターンオン動作時のゲート電圧V_{GE}とコレクター電流I_Cに対して様々な決定方法が提案されている[(1)(2)(3)]。この開発でのデジタルゲート駆動技術はゲート駆動信号の強度を“強，弱(高インピーダンス)，強”と３回変化させる駆動方法である。この開発では駆動信号の強度を変化させるタイミングt_1とt_2を求める新たな方法を提案し，汎用のゲートドライバーICを用いてt_1とt_2のそれぞれを変化させた評価結果からその妥当性を検証した。

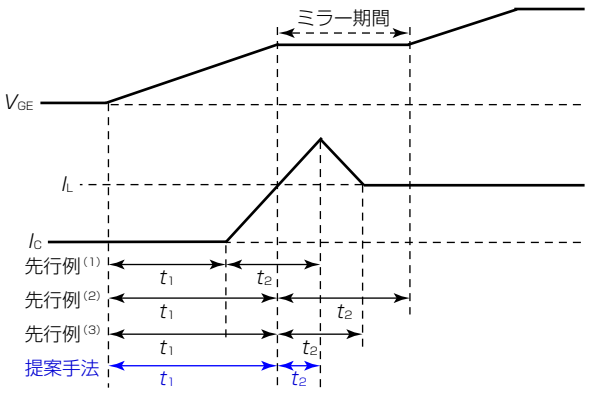
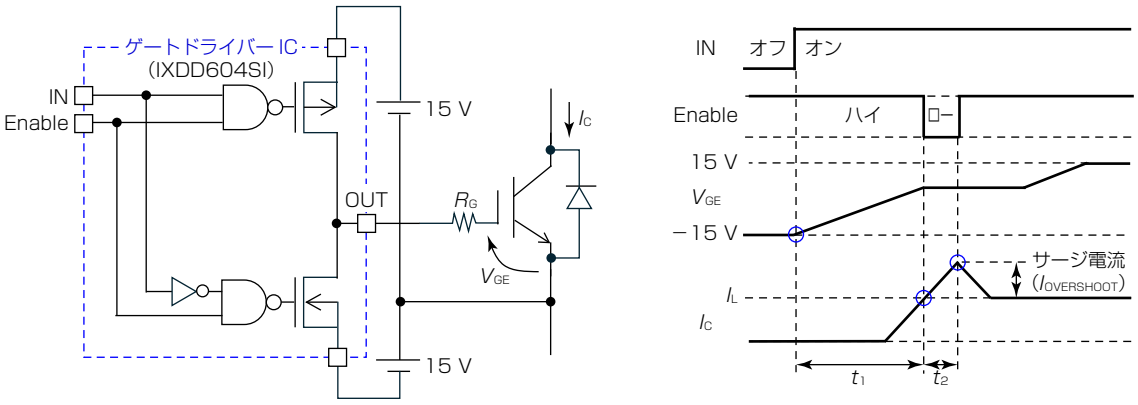


図１－ターンオンでの様々なt_1とt_2の決定方法

2. 提案する最適な駆動タイミングの決定手法

図２に提案手法での回路図とタイミングチャートを示す。Enable付きのゲートドライバーIC(IXDD604SI)を使用し，タイミングチャートのt_1とt_2は入力信号INとEnable信号のタイミングを制御する。Enable信号がローのとき，出力OUT

は高インピーダンスになる。提案手法のt_1はV_{GE}の立ち上がりエッジからI_Cが負荷電流I_Lになるまでの時間である。t_2はI_Cが負荷電流I_Lになったときからピーク値になるまでの時間であり，パワーモジュールの動作条件が変わるとt_1とt_2も変化する。提案手法のt_1とt_2は，測定したV_{GE}とI_Cの波形から算出する。



(a)　回路図　　(b)　タイミングチャート

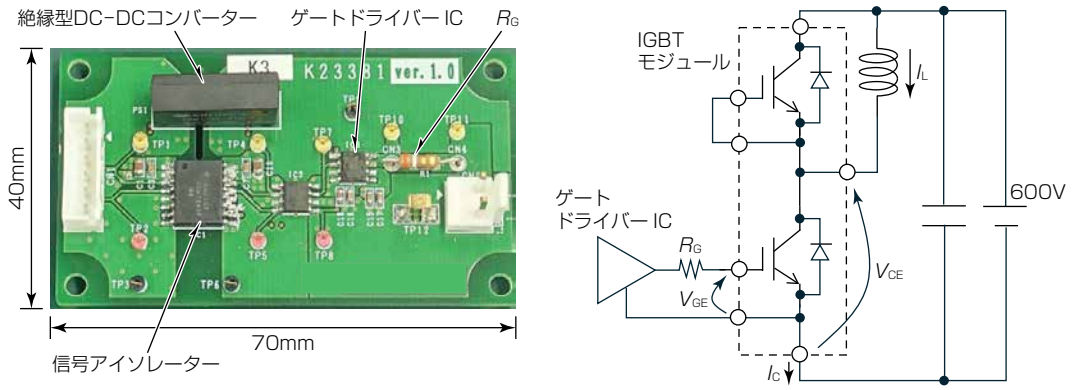
図２-提案手法の回路図とタイミングチャート

従来のゲート駆動回路(以下“従来手法”という。)では，ゲート抵抗R_Gを変化させながらスイッチング損失E_{LOSS}とサージ電流$I_{OVERSHOOT}$のトレードオフカーブを取得する。提案手法での損失低減率を式(1)で定義する。$E_{LOSS,\ DGD}$は提案手法でのスイッチング損失である。$E_{LOSS,\ CONV}$は従来手法でのスイッチング損失であり，提案手法と同程度のサージ電流で比較するため，従来手法で取得したトレードオフカーブの近似曲線から計算する。

$$\text{損失低減率} = \frac{E_{LOSS,\ CONV} - E_{LOSS,\ DGD}}{E_{LOSS,\ CONV}} \times 100 \quad \cdots\cdots (1)$$

3. 評 価 方 法

図３にゲートドライバー基板とスイッチング評価の回路図を示す。ゲートドライバー基板は信号アイソレーターと絶縁型DC-DCコンバーターを搭載する。評価対象にはIGBT(Insulated Gate Bipolar Transistor)モジュール(CM100DY-24T, 定格：1,200V，100A)を用いた。提案手法と従来手法，及び先行例[1][2][3]で提案されているt_1とt_2の決定手法でそれぞれ測定した。提案手法ではt_1とt_2を2ns間隔で2,400通りの組合せで依存性を測定し，提案手法の妥当性を検証した。

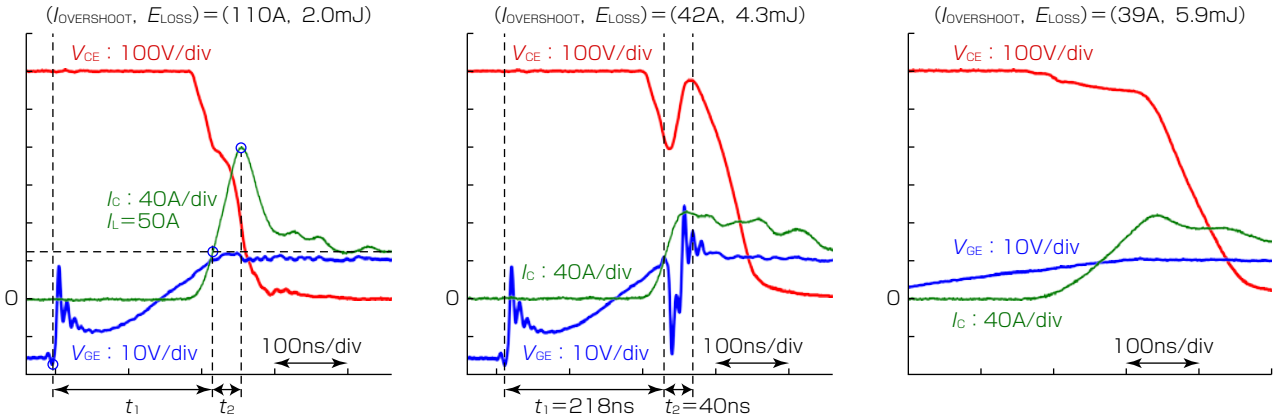


(a)　ゲートドライバー基板　　(b)　スイッチング評価の回路図

図３-ゲートドライバー基板とスイッチング評価の回路図

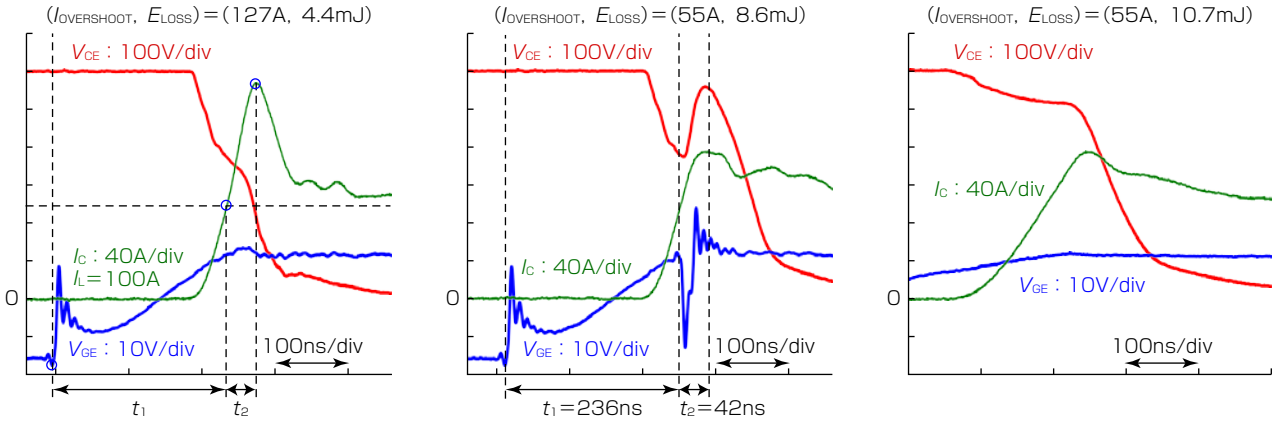
4. 評 価 結 果

図4と**図5**に負荷電流I_L＝50Aと100Aでの提案手法と従来手法のスイッチング波形をそれぞれ示す。これらのスイッチング波形からスイッチング損失とサージ電流を求めて，先行例[1][2][3]の結果を含めて相反関係を比較する。提案手法のt_1とt_2は従来手法のゲート抵抗R_Gを3.9Ωとしたときのスイッチング波形から算出した。**図6**が負荷電流I_L＝50Aと100A



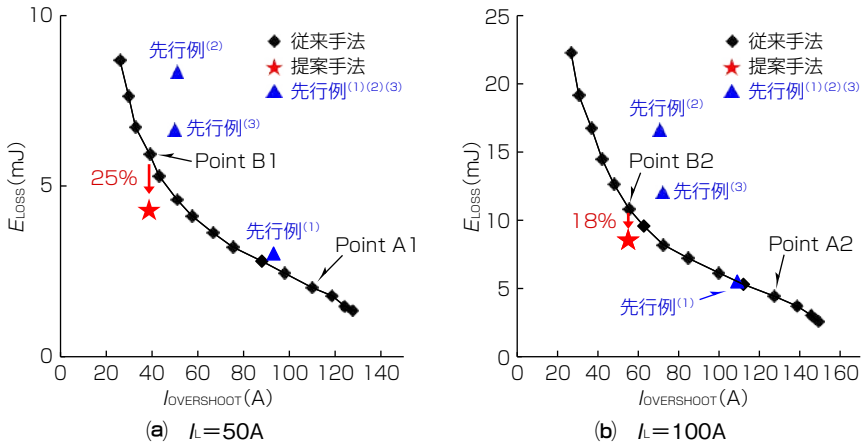
(a)　従来手法Point A1（R_G＝3.9Ω）　(b)　提案手法　(c)　従来手法Point B1（R_G＝18Ω）

図4－I_L＝50Aでの提案手法と従来手法のスイッチング波形



(a)　従来手法Point A2（R_G＝3.9Ω）　(b)　提案手法　(c)　従来手法Point B2（R_G＝12Ω）

図5－I_L＝100Aでの提案手法と従来手法のスイッチング波形

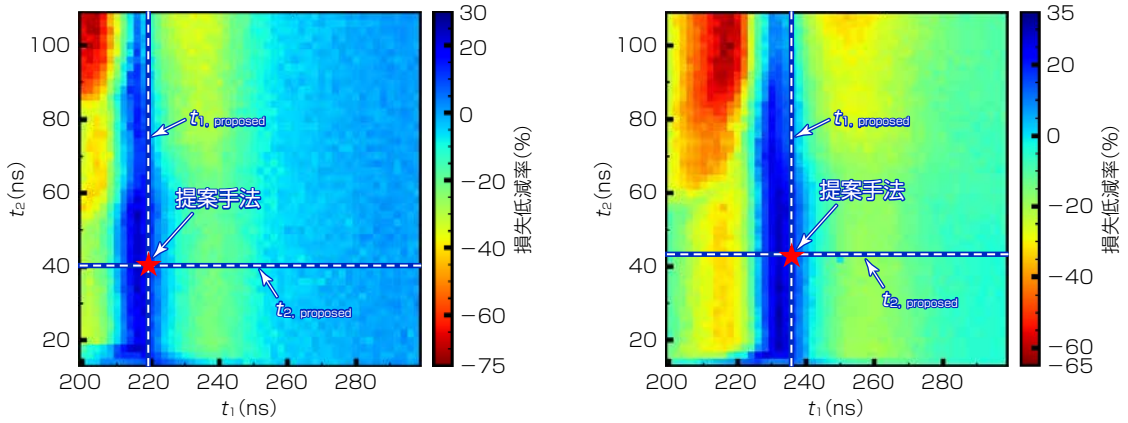


(a)　I_L＝50A　(b)　I_L＝100A

図6－スイッチング損失E_{LOSS}とサージ電流$I_{OVERSHOOT}$の評価結果

での提案手法と従来手法，及び先行例[1][2][3]でのスイッチング損失E_{LOSS}とサージ電流$I_{OVERSHOOT}$の評価結果である。提案手法では，サージ電流$I_{OVERSHOOT}$を従来手法と同程度に維持しつつ，負荷電流I_L＝50Aではスイッチング損失E_{LOSS}を25%，100AではE_{LOSS}を18%低減した。なお，先行例[1][2][3]では従来手法よりもE_{LOSS}が増大する結果になった。

図7に負荷電流I_L＝50Aと100Aでの損失低減率のt_1とt_2の依存性を示す。損失低減率はt_1依存性が非常に大きくt_2依存性は小さいことから，t_1の最適化が重要であることが分かる。提案手法では，損失低減率への影響が大きいt_1の最適値を得ることができて，先行例[1][2][3]よりも損失の低減効果が高い結果を得ることができた。**表1**に温度T_jを25℃と75℃，及び125℃としたときの提案手法と先行例[1][2][3]での損失低減率の評価結果を示す。温度T_jを75℃と125℃とした条件下でも，提案手法は先行例[1][2][3]よりも損失の低減効果が高くなることを確認した。



(a)　負荷電流I_L＝50A　　(b)　負荷電流I_L＝100A

図7－損失低減率のt_1とt_2の依存性

表1－提案手法と先行例[1][2][3]の損失低減率

	I_L＝50A			I_L＝100A		
	T_j＝25℃	T_j＝75℃	T_j＝125℃	T_j＝25℃	T_j＝75℃	T_j＝125℃
提案手法(%)	25	23	16	18	26	27
先行例[1](%)	−20	−10	−9	0	−2	−1
先行例[2](%)	−84	−64	−50	−95	−96	−70
先行例[3](%)	−43	−75	−64	−45	−78	−90

5. むすび

デジタルゲート駆動技術で，駆動信号の強度を変化させるタイミングを決定する新たな方法を提案した。提案手法の損失の低減効果が最も高く，その妥当性を実証した。

今後，提案手法の実用化に向けて継続して開発を進めて，パワエレ機器の省エネルギー化に貢献する。

参考文献

(1) Zhang, F., et al.：Advanced Active Gate Drive for Switching Performance Improvement and Overvoltage Protection of High-Power IGBTs, IEEE Transactions on Power Electronics, **33**, No.5, 3802～3815 (2017)
(2) Camacho, P.A., et al.：A Novel Active Gate Driver for Improving SiC MOSFET Switching Trajectory, IEEE Transactions on Industrial Electronics, **64**, No.11, 9032～9042 (2017)
(3) Manuel, R., et al.：Implementation of Current-Source Gate Driver with Open-Loop Slope Shaping for SiC-MOSFETs, International Exhibition and Conference for Power Electronics,Intelligent Motion, Renewable Energy and Energy Management, 1～8 (2021)

特集論文

生産現場の運用自動化を支えるシステム制御計画作成技術

中井敦子* Atsuko Nakai
海江田広和* Hirokazu Kaieda
矢口喬脩* Takanobu Yaguchi
中川晃一* Koichi Nakagawa
八田夏美* Natsumi Hatta

*先端技術総合研究所

Making Control Plans to Automate System Operations in Manufacturing Site

要　旨

生産現場では，労働力不足を補うための運用自動化ニーズが高まっている。生産現場での生産スケジュールは現場監督者が作成することが多いが，非常に労力がかかる作業になっていた。この課題を解決するために，現場作業者と生産設備が混在して作業する生産現場で生産能力が低下した際に，現場作業者と生産設備各々についてあらかじめ定義したプロファイル情報を用いて最もコスト効率の高い対策を自動立案し，適用する手法を開発した。また，生産設備での非稼働時間を最小化する生産スケジュールを高速に作成するために，整数最適化問題として定式化し処理する部分とルールベースで処理する部分を組み合わせた最適化手法を開発した。

1. ま え が き

近年，日本の生産現場では，生産年齢人口の減少や消費者ニーズの多様化による多品種少量生産への転換等，生産技術の革新が求められている(1)。特に，食品工場や物流現場等では，夜間や休日の操業が不可欠であり，労働力の確保を更に困難なものにしている。労働力不足を補うために，生産設備の自動化が進められており，現場作業者の省人化による労働力の安定確保や作業負担軽減による生産効率の向上が見込まれる一方，生産設備と現場作業者の性能差が大きくなって，製造ラインの性能を保つことが困難になるという課題が生じている。また，生産の効率化を狙って，現場監督者が勘と経験によって生産スケジュールを作成しているが，これが現場にとって大きな負担になっていた。これらの課題を解決するために，現場作業者と生産設備が混在する生産現場で生産能力低下時に最適な対策を自動立案・適用する手法を考案した。具体的には，現場作業者と生産設備それぞれについてあらかじめ定義したプロファイル情報を活用し，最もコスト効率の高い対応策を自動的に導出する方式を開発した。また，生産設備での非稼働時間を最小化する生産スケジュールを高速に作成するために，考慮すべき多数のパラメーターを整数最適化問題として定式化し処理する部分とルールベースで処理する部分に分けて組み合わせることで，数十秒以内での生産スケジュール作成を実現した最適化手法を開発した。生産現場が要求する制約条件のうち，変動性の高い制約条件を整数最適化問題として定式化し，ソルバーを用いて解を求める。次に，生産現場に汎用的な制約条件をルールベースのアルゴリズム処理としてソルバーで求めた解に適用することで，生産スケジュールを作成する。

2. 生産設備と現場作業者のプロファイル情報を用いた生産システム運用制御方式

この章では，生産設備と現場作業者それぞれについて定義したプロファイル情報を用いて自動的に制御指令を作成する方式について述べる。提案方式は，ロボットや自動搬送機，制御装置等で構成される生産設備のプロファイル情報と，ステータス値やセンサー値，操作履歴等を含む作業者のプロファイル情報とを逐次的に収集・分析し，過去に同様の作業を実施した際のプロファイル情報と比較する。場の状況に応じて，生産設備や現場作業者のプロファイル情報をどのように変化させる又は変化させないことで所望の性能に到達するかをシミュレーションする。そして，所望の性能を実現するための制御内容を決定し，作業者と生産設備に対して配信することを目的としている。

プロファイル情報とは，生産設備固有の情報又は現場作業者固有の情報である属性情報と，生産システムの中で生産設備又は現場作業者が発揮する作業能力に関する情報である性能指標情報とで構成される。すなわち，プロファイル情報は，現場作業者と生産設備による総合的な作業能力を示す情報と定義する。生産設備としてロボットを例に具体的なプロファイル情報項目例を示すと，属性情報としてはカタログスペック値のほかに，“設置ライン名”などのロボットの運用に関わる情報がある。また，性能指標情報としては，作業対象物ごと又は作業条件ごとに算出される“作業速度”又は“作業不良

発生率”などの実稼働データから算出される情報を含む。現場作業者に対応するプロファイル情報項目例を示すと，属性情報としては人事情報や従事する業務内容に関わる情報などがある。また，性能指標情報としては，生産設備の場合と同様に，作業内容ごと又は作業条件ごとに算出される“作業速度”又は“作業不良発生率”などの実稼働データから算出される情報を含む。プロファイル情報は，工場種別や導入設備の違い等によって異なる部分もあるが，最低限の標準化を行う必要がある。そのため，プロファイル情報のひな型として，OPC UA(注1)の情報モデルやコンパニオン仕様を活用することとした。例えば，ロボットに対してはOPC UA for Roboticsが策定されている。これらの情報モデルを基に，プロファイル情報に関連する項目を追加・拡張させることで，プロファイル情報の標準化を実現するとともに，プロファイル情報の収集や評価にかかるコストを低減できる。

この方式は，工場内に設置されたエッジプラットフォーム端末を中核にして動作するように設計した。**図１**にシステム構成を示す。エッジプラットフォーム端末内には，生産現場のデータ収集・加工・配信等を汎用的に行うために，一般社団法人 Edgecrossコンソーシアムが提供するエッジコンピューティング領域のオープンなソフトウエアプラットフォームであるEdgecross(注2)(2)を採用した。今回は，OPC UA対応の生産設備や他システムとEdgecrossの間でプロファイル情報を共有し，OPC UAのAPI(Application Programming Interface)を用いて互いに配信する仕組みとした(3)。

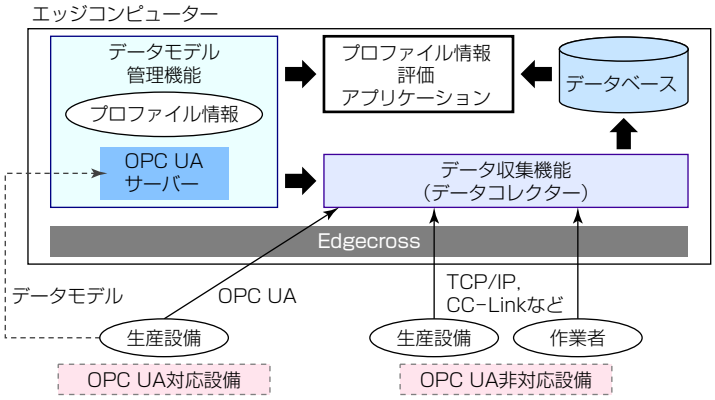


図１-システム構成

今回，エッジプラットフォーム端末内部にプロファイル情報評価アプリケーションを作成した。このアプリケーションは，Edgecrossで収集したプロファイル情報を逐次評価し，生産システムの性能低下が見込まれる場合に，あらかじめ管理者が設定した評価指標のうち向上効果の高いプロファイル情報項目を変化させるための制御指令を出したときの効果をシミュレーションする。仮想的に生成した作業者及び生産設備のプロファイル情報値に基づいて，逐次的に分析を行い，性能低下を予測できるか，また，性能改善のための制御指令を作成できるかを検証するアプリケーションを試作し，市販のエッジコンピューター上で検証を実施した。**図２**に試作した検証画面例を示す。

図２-生産システム運用制御方式の検証画面例

この例では，２台のピッキングロボットと複数の作業者が弁当の具材を詰める作業ラインで，Edgecrossで具材残量やロボットの稼働状況を収集する状況を模している。具材残量を予測しながら，具材残量が０になってラインが停止することのないようにあらかじめ制御指令を作成できるかを検証した。その結果，ほぼ遅延なくプロファイル情報の評価と制御指令の作成が可能であることを確認できた[4]。

（注１）　産業オートメーション分野で，異なるメーカーの機器やシステムが安全かつ確実にデータを交換するための国際標準規格。OPC UAは，OPC Foundationの登録商標である。
（注２）　Edgecrossは，一般社団法人 Edgecrossコンソーシアムの登録商標である。

3. 処理優先度を考慮した並列機械工程スケジューリング方式

この章では，多品種少量生産を行う生産現場で，複数の生産設備に対する生産スケジュールを高速に作成する手法を提案する。

3.1 問 題 設 定

想定したスケジューリング問題の前提条件について述べる。生産設備がm台稼働している生産現場で，n個の“ジョブ”と呼ばれる生産工程が実行待ちになっている状態を仮定する。各ジョブjはどの順番で実行してもよく，また，どの生産設備で処理してもよい。各ジョブjの処理時間l_jは使用する生産設備によって変化しない。また，その処理時間の最大値は23時間以内と定義する。各ジョブjには，ジョブが実行完了されていることが望ましい期日として，納期d_jがそれぞれ設定されている。各ジョブjは１台の生産設備で処理できる単位で作られている。ジョブの種類としては，事前に作成する“通常ジョブ”に加えて，処理失敗や処理が不十分な場合等に急きょ作成する“割り込みジョブ”の２種類があり，各ジョブはそのいずれかに該当する。これらの前提条件に基づいて，次のように制約条件を設定する。

制約①納期遅れ和最小化：各ジョブjに設定される納期d_jは日単位で設定される。納期d_jとスケジューリング後の処理日との差を“納期遅れ”として定義し，処理日が納期前であれば納期遅れは０とする。各ジョブの納期遅れの総和が小さくなるようにスケジュールを作成する。

制約②優先度制約　：割り込みジョブにはそれぞれ優先度pを設定し，優先度が高いものからスケジューリングされる。通常ジョブは全ての割り込みジョブが処理完了する日時以降でスケジューリングされる。

制約③稼働時間制約　：各生産設備iにはそれぞれ稼働時間上限t_iを決めることができる。その場合，各生産設備iが処理する各ジョブの処理時間の合計はt_iを超えない。

制約④負荷分散制約　：各生産設備iで処理するジョブの総処理時間がおおよそ均一になるように負荷分散を考慮したスケジュールを作成する。

制約⑤逐次実行制約　：各生産設備iで処理するジョブは逐次的に実行される。

3.2 提 案 手 法

ここでは，**3. 1節**で述べた前提条件の下，制約条件を満たすスケジュールを求める手法として，整数最適化問題で定式化する部分とルールベースのアルゴリズムで処理する部分に分ける方針とした。

整数最適化処理部分は，**3. 1節**で述べた前提条件と制約①から制約④までの制約条件を整数最適化問題として定式化する。制約②と制約③は求めるスケジュールが必ず満たすべき条件であるため，絶対制約として最適化問題での制約条件式に組み込む。制約①と制約④は更に良い解を得るために満たすことが望ましい条件であるため，考慮制約として，最適化問題での目的関数に組み込む。定式化は次のとおりになる。

$$x_{ij}=\begin{cases}1(\text{生産設備}i\text{にジョブ}j\text{を割り当て})\\0(\text{otherwise})\end{cases} \quad \cdots\cdots(1)$$

$l_j \in \mathbb{Z}$：ジョブjが生産設備で処理される時間 ……(2)

J：全てのジョブの集合 ……(3)

$d_j \in \{0,\ 1,\ 2,\ \cdots\}$：ジョブ$j$の納期までの日数 ……(4)

t_i：生産設備iの最大稼働時間 ……(5)

$p \in \{1,\ 2,\ \cdots\}$：各ジョブjに設定された優先度 ……(6)

$J_p \subseteq J$：優先度pのジョブの集合 ……(7)

$b_p \in \{0, 1\}$：優先度制約に関する補助変数 ……(8)

$e_j = f(d_j)$：納期遵守に対する利得 ……(9)

minimize $-P_1 - P_2$ ……(10) 制約①＋制約②の目的関数

subject to $P_1 = \Sigma_i \Sigma_j x_{ij} e_j$ ……(11) 制約①納期遅れ和最小化

$P_2 = y$ ……(12) 制約④負荷分散制約

$y \leq \Sigma_{j \in J} l_j x_{ij} (i = 1, 2, \cdots, m)$ ……(13) 制約④負荷分散制約

$\Sigma_{j \in J} l_j x_{ij} \leq t_i (i = 1, 2, \cdots, m)$ ……(14) 制約③稼働時間制約

$\Sigma_i x_{ij} \leq 1 (j = 1, 2, \cdots, n)$ ……(15)

$b_p \geq b_{p+1} (p = 1, 2, \cdots)$ ……(16) 制約②優先度制約

$\Sigma_i x_{ij} \leq b_p (j \in J_p, p = 1, 2, \cdots)$ ……(17) 制約②優先度制約

$b_{p+1} \leq \Sigma_i x_{ij} (j \in J_p, p = 1, 2, \cdots)$ ……(18) 制約②優先度制約

続いて，ルールベース処理部分について述べる。**3. 1節**で述べた各制約条件のうち，制約⑤をルールベースのアルゴリズムで処理する。具体的には，式(1)～(18)で表現した整数最適化問題を解くことによって得られる，各ジョブと処理する生産設備との対応関係を用いて各生産設備の時系列スケジュールを作成する処理を，ルールベースのアルゴリズムを用いて実行する。用いるアルゴリズムを次に示す。

Step１：各生産設備に割り当てられたジョブを集める。

Step２：集めたジョブのうち，割り込みジョブを優先度が高い順に並べる。優先度が同一の場合は納期に余裕がないジョブから並べる。

Step３：全ての割り込みジョブの後に，通常ジョブを納期に余裕がないジョブから順に並べる。

Step４：並べたジョブと時間軸を対応させることで時系列に並んだ生産スケジュールを作成する。

3. 3　数 値 実 験

生産現場での標準的な放電加工工程を模したジョブを用意し，それらを提案手法に適用することによって，生産スケジュールを求める数値実験を行った。実験方法について述べる。用意するジョブは幾つかのテストケースを想定して作成し，それぞれに対して想定例となる生産スケジュールをあらかじめ求めておく。各テストケースに対して提案手法を適用することで求めたスケジュールと想定例のスケジュールを比較し，提案手法の有効性を確認する。

今回の数値実験は，次に示す設定で実施した。

①スケジュール作成期間　　：７日間
②稼働加工機台数　　：３台
③各加工機の１日当たりの稼働時間：23時間
④各テストケースの実験回数　　：20回
⑤スケジューリング実施単位　　：１日
⑥実験パソコンのCPU　　：11th Gen Intel Core(注3) i5-1145G7@2.60GHz
⑦実験パソコンのメモリー　　：16GB

スケジューリング実施単位とは，提案手法を１回適用することによって求めるスケジュールの期間である。今回の数値実験では，日付をまたぐジョブが発生しないようにするために，スケジューリング実施単位を１日とした。

テストケースは次のような三つの例を用意し，それぞれ想定例となるスケジュールを作成した。Case１，Case２，Case３の順に，より難易度が高くなるようにテストケースの設計を行った。

Case１：１日分として処理時間の和が23時間になるようにジョブを作成する。これをスケジュール作成期間，及び稼働加工機台数だけ用意する。このとき，各ジョブの優先度は同一である。また，想定例で各日にスケジューリングされるジョブはその日が納期になっている。また，各ジョブの処理時間は60分の倍数とする。

Case２：Case１で作成した各ジョブについて，優先度を設定する。

Case３：Case２で作成した各ジョブに，処理時間が60分で割り切れない“500分”のジョブを稼働加工機台数分追加する。“500分”のジョブの納期は７日目として，一つでもスケジューリングすると１日当たり23時間分のジョブを隙間なく計画できなくなるため，納期違反が発生することが予想される。

各テストケースの想定例として，１日分のスケジュール例を**図３**に示す。

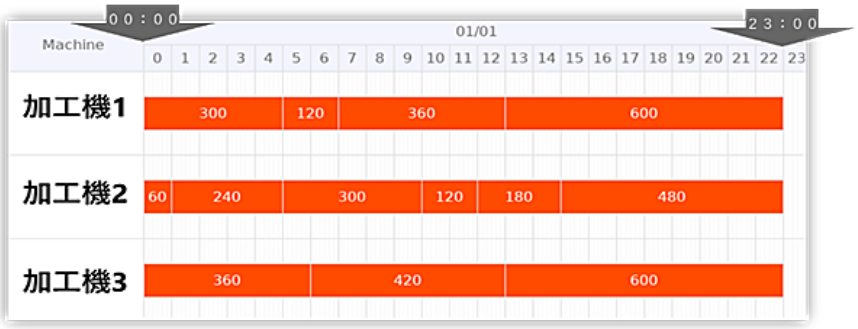


図３-並列機械工程スケジューリング方式の想定例

図３は３台の加工機の１日のスケジュール例を示す。横軸が１時間ごとの時間軸，縦軸が各加工機のスケジュール結果である。上から加工機１，加工機２，加工機３で，割り込みジョブは赤色，通常のジョブは青色で表記している。また，各ジョブの矩形(くけい)内の数値は加工時間(分)を表す。このように想定例では０時から23時まで空き時間のないスケジュールを作成できる。したがって，提案手法で求めたスケジュールに空き時間が存在しなければ，想定例と同様の最適解を得ることができたと考えられる。提案手法で求めたスケジュールに空き時間が存在する場合，求めたスケジュールがどの程度最適解に近いかを想定例との乖離(かいり)程度から評価することにして，次のような評価指標を設定した。どの指標も，想定例と同等又はそれ以下であることが評価条件になる。

①納期違反数　：各ジョブをスケジューリングした結果，あるジョブが加工される計画日がそのジョブの納期よりも後である場合，納期違反になる。この納期違反を各ジョブに対して検査することで求めた納期違反数を評価指標とする。

②納期違反量　：各ジョブをスケジューリングした結果，あるジョブが加工される計画日がそのジョブの納期よりも後である場合，そのジョブの加工時間を納期違反量とする。ただし，計画日が納期より前である場合は納期違反量が０であるとする。このとき，各ジョブの納期違反量の総和を取ったものを評価指標とする。

③演算時間　　：生産現場ではスケジューリングで許容できる時間に制限があることが多いため，上限を60秒として，この上限以内に計算が終了しているか否かを評価指標とする。

式(11)で，最小化している納期遅れ和は上記評価指標のうち，納期違反数と納期違反量で評価する。これは，納期遅れが１日単位で算出されるため，加工時間の大きいジョブが納期遅れになっても，加工時間の小さいジョブが納期遅れになっても同一評価になることを防ぐためである。提案手法によって求めたスケジュール，想定例のスケジュールのそれぞれに対して，これらの評価指標で評価を行い，その差を用いて提案手法によって求めたスケジュールが妥当であるかを検証する。

テストケース(Case１～３)に対して，提案手法を適用することによって求めたスケジュールが制約①納期遅れ和最小化～⑤逐次実行制約を満たしているかを検証する。まず，提案手法を各テストケースに適用することで，生産スケジュールを求める。次に，これらの求めた生産スケジュールに対して，各評価指標に基づいて評価値を算出する。この評価結果を**表１**に示す。各評価指標の値は，20回のスケジューリングを実行して得られたデータの平均値である。

表１-各評価指標での提案手法の評価結果

	Case 1	Case 2	Case 3
納期違反数	0	0	3
想定例での納期違反数	0	0	3
納期違反量(分)	0	0	1,500
想定例での納期違反量(分)	0	0	1,500
平均演算時間(秒)	1.836	1.970	2.589

表１に示すように，Case１～３の全てのテストケースで，あらかじめ作成しておいた想定例と比較すると，全ての評価指標が想定例と同等のスケジュールを得た。また，最も複雑なテストケースであるCase３で，**表１**には表れない制約②優先度制約の条件が満たされているかを確認するために，作成されたスケジュールを図示したものを**図４**に示す。**図４**

は，提案手法によるスケジューリング結果のうち，７日目と８日目を抜粋したものである。７日目以前のスケジュール期間内に“500分”のジョブがスケジューリングされた場合，想定例での各評価指標の値よりも悪化することが考えられる。しかし，**図４**の結果では想定したスケジュールと同等であり，各評価指標の値も同等であることが確認できた。また，**図４**上部に表示した１～８日目のスケジューリング結果全容を見ると，１～３日目には，割り込みジョブを表す赤色のジョブが固まっており，通常のジョブを表す青色のジョブは４日目以降に固まってみられることから，制約②優先度制約も満たされていると言える。以上の結果から，式(1)～(18)によって，最適スケジュールを作成できたと考えられる。すなわち，提案手法は，ジョブ数が少ない簡単なテストケースで，最適なスケジュールを求めるという基本性能を持っていることが確認できた[5]。

（注３）　Intel Coreは，Intel Corp.の登録商標である。

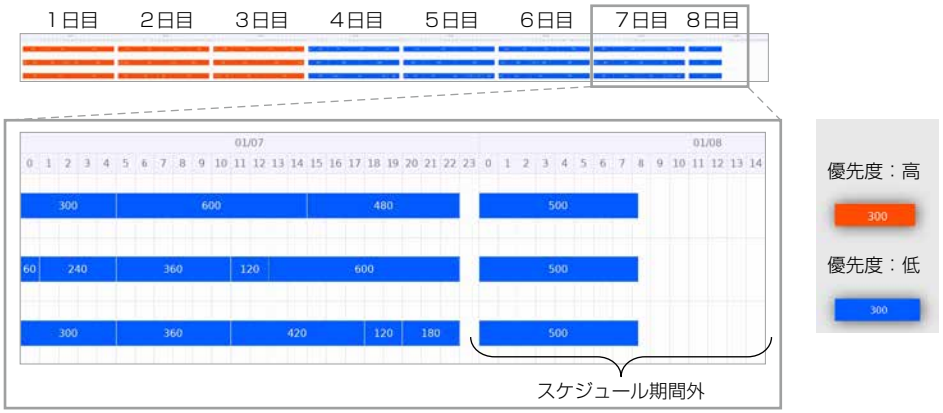


図４-Case３のスケジューリング結果（７～８日目）

4. む　す　び

生産現場で，現場作業者と生産設備とが混在している状況で，運用を自動化するための手法として，ライン稼働データをエッジプラットフォームで収集・分析することによってライン全体の統合監視を行う性能プロファイル連携制御方式と，生産現場で高速に工程実行順序を決定するために，制約条件を整数最適化処理部分とルールベース処理部分とに分けたことを特徴とする工程スケジューリング方式について述べた。どちらの方式も生産現場で要求される秒単位での計画作成を達成できた。

参 考 文 献

(1)　産業競争力懇談会COCN：「人」が主役となる新たなものづくり，産業競争力懇談会 2017年度 プロジェクト 最終報告（2018）
http://www.cocn.jp/report/theme97-L.pdf
(2)　一般社団法人 Edgecrossコンソーシアム：Edgecross Consortium
https://www.edgecross.org/ext/ja/index.html
(3)　中井敦子：エッジプラットフォームを用いたROSと生産システムとの連携方式に関する一検討，2022年電気学会電子・情報・システム部門大会，OS1-6（2022）
(4)　中井敦子：作業者と生産設備とのプロファイル情報を用いた生産システム運用制御方式の検討，第22回情報科学技術フォーラム，J-022（2023）
(5)　矢口喬脩，ほか：処理優先度を考慮したFA向け並列機械工程スケジューリング，2023年電気学会電子・情報・システム部門大会，OS1-2-5（2023）

特集論文

トレーラー自動搬送でのトラクターの認知技術と自動運転制御技術

本間　充*
Mitsuru Homma
秋山智広*
Tomohiro Akiyama
藤好宏樹*
Hiroki Fujiyoshi
山田浩史*
Hiroshi Yamada

*先進応用開発センター

Recognition Technology and Autonomous Driving Control Technology for Tractors in Automated Trailer Transportation

要　旨

三菱電機は，労働力不足やコスト上昇といった物流業界の課題に対応するため，物流倉庫内のトレーラー自動搬送でのトラクターの認知技術と自動運転制御技術の開発に取り組んでいる。この技術は，緊急自動ブレーキ機能や複数センサーを活用したセンサーフュージョン技術が搭載されたトラクターによって，自動搬送と施設全体の運用効率及び安全性を高めることができる。さらに，トレーラーの搬送指示に基づいてトレーラー牽引(けんいん)状態と自動運転タスクに応じた経路生成手法を適切に切り替える経路生成管理機能を導入し，トラクターの自動運転制御を高精度かつ効率的に実現している。

1. ま え が き

米国の物流業界では，ドライバー不足とそれに伴う人件費高騰による事業継続リスクといった課題が生じている。特に大型物流倉庫ではドライバーが昼夜問わずトラクターを運転して荷物を積載したトレーラーを搬送していることから，24時間365日，無人かつ安全にトレーラーを搬送するソリューションが求められている。当社はこの課題を解決するため，物流倉庫内のトレーラー自動搬送でのトラクターの認知技術と自動運転制御技術を開発している(**図1**)。

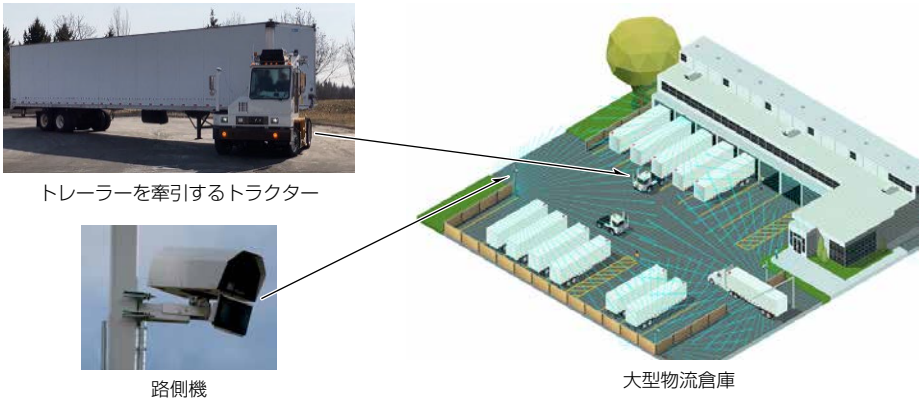


図1－トレーラー自動搬送

路側機は，入門ゲートに配置された複数のカメラと施設内全領域をカバーする複数のLiDAR(Light Detection and Ranging)を用いて，主に障害物検出を行う。障害物検出機能は，施設内の事故リスクの低減を目的としている。この機能は，施設内に搭載している全てのLiDARの情報を用いて，施設内の障害物の位置・速度・サイズ・属性(歩行者・車・トレーラーなど)を検出する。障害物情報はトラクターに送信されて，必要に応じてトラクターを減速又は停止させることができる。

トラクターの認知技術によって，トラクター周辺の状況を監視する多種のセンサーを組み合わせて，物体の位置を天候の変化によらず高精度に検出する。また，トラクターの自動運転制御技術によって，トラクターがトレーラーを牽引しながら走行してトレーラーを指定される位置に搬送する。そのために，トラクターとトレーラーの運動を考慮して前進又は後退を可能にする走行経路を生成し，その走行経路に対してトラクターを高精度に制御する。またトレーラーの移動時間を最小化するために，トレーラーの搬送指示に基づいて，複数ある走行経路生成手法を最適に組み合わせたり，最短距離になる走行経路を計画したりする。さらに，認知した障害物との衝突可能性を判断して自動ブレーキを作動する。

2. トラクターの認知技術

トラクターには，自動運転時の安全を確保するために緊急自動ブレーキシステムを備える。自トラクターの周囲(距離30m，周囲360度)に存在する人や他トラクターなどの障害物を検知し，衝突の危険性がある場合には自動でブレーキをかけるシステムである。雨・雪・路面形状などの外部環境に対しても信頼度高く検知するロバスト性，障害物を精度良く検知する冗長性，トレーラー牽引有無など検知対象に対する柔軟性，などの高い要求性能が求められていた。この課題に対応するために，異なる特徴を持つセンサーを搭載する。具体的には，空間分解能と測距精度に優れているLiDARと，人物検知が得意なカメラ，さらに雨天や降雪時などの悪天候時でも検知性能が低下しないミリ波レーダーを用いて自トラクター周囲の障害物を検知する。そして，これら複数センサーの検知結果を融合するセンサーフュージョン技術をソフトウエアに実装することによって要求性能を達成した。

ソフトウエア開発では，現実世界で取得したセンサーデータを用いた検証とシミュレーションによる検証を行った。シミュレーション検証では，トラクター運動と周囲環境，さらにセンサーの結果をバーチャル空間に再現し，センサーフュージョン技術を検証可能な環境を構築した(**図２**)。網羅的な検証パターンの作成と自動検証機能を実現し，現実世界ではデータ取得が難しい環境や試験条件での検証も可能にすることで，ソフトウエア開発効率と開発速度を大幅に高めた。

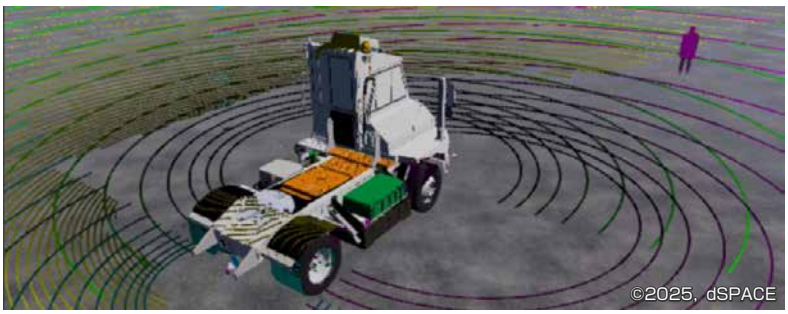


図２-トラクターの認知技術のシミュレーション動作例

3. トラクターの自動運転制御技術

トラクターは，自動運転タスクの一例として，複数の駐車枠が存在する駐車場で，駐車枠Aから走行を開始し，駐車枠Bに駐車するトレーラーに接続した後，そのトレーラーを牽引して駐車枠Cへ搬送することが求められる(**図３**)。これらの自動運転タスクで，トラクターはトラクター単独の運動，又はトラクターと牽引するトレーラーの両者の運動を考慮し

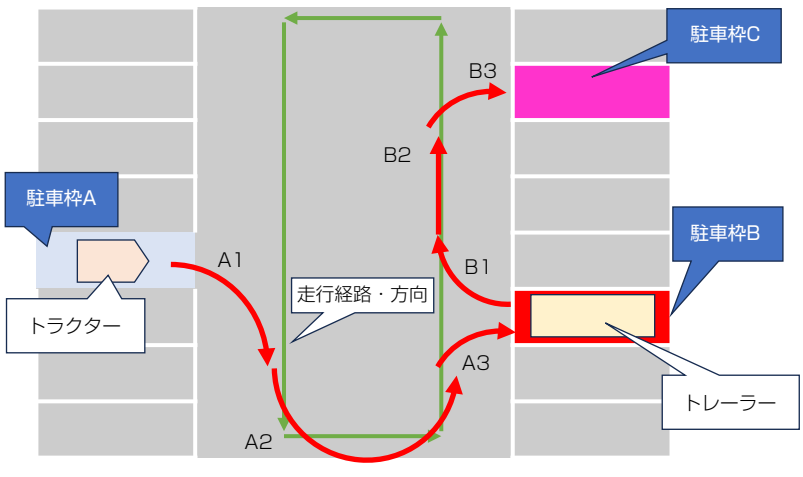


図３-トラクターの自動運転制御技術が実行する自動運転タスクの一例

て制御する。また駐車枠に停車するトレーラーに対してトラクターを連結したり，トレーラーを指定される位置に移動したりするために，トラクターは前進後退しながら高精度に位置制御することが求められる。これまで当社はトレーラーの牽引有無や前進後退に応じた最適な経路生成手法を開発しており，それら複数の経路生成手法を適切に切り替えて管理することで自動運転タスクを実行する。

この章では，複数の経路生成手法を選択する必要性，経路生成管理機能の動作を詳細に述べた後，机上での検証結果を述べる。

3.1　経路生成手法切替えの必要性

トレーラーの牽引有無に応じて，前進後退を切り替えながら目標位置に到達する経路生成として，Leuらが提案した手法(improved A-Search Guided Tree：i-AGT)[1]が考えられる。しかしi-AGTを単独で用いる場合，常にトレーラーの牽引を考慮した経路生成になるため，目標位置に到達する経路が大回りになる可能性がある。またi-AGTは探索空間内で開始位置から目標位置までの経路をグラフ探索する手法であるため，広範囲で経路生成する場合，探索空間が増大してメモリー消費量と計算量が増加する問題が生じる。これらの理由から，i-AGT単独ではなく，複数の経路生成手法の切替えが必要になった。そこで，Iqbalらが提案するトラクター単体のパーティクルフィルター(Particle Filter)ベースの経路生成をトレーラー牽引状態に拡張した経路生成手法(Particle Filter Motion Planner：PFMP)[2]及びWangらが提案するヒッチングのための経路生成手法(Bi-Directional A-Search Guided Tree：BIAGT)[3]を用いた。

さらに前進後退で用いるBIAGT又はi-AGTの計算時間は，PFMPよりも長く，経路生成する走行距離に依存する。そこで経路生成に要する計算時間を最小化するために，計算時間が短いPFMPが経路生成する距離を最大化し，BIAGT又はi-AGTによって経路生成する距離を最小化した。

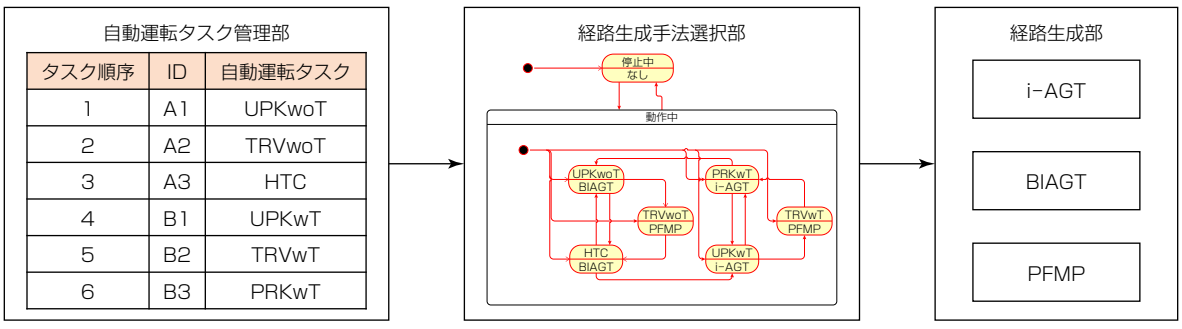
経路生成手法に応じたトラクターの走行動作を自動運転タスクとして，経路生成手法との対応関係を**表1**に示した。

表1-自動運転タスクと経路生成手法の対応関係

ID	自動運転タスク	経路生成手法
A1	トラクター単体で駐車枠Aから走行経路に復帰	BIAGT
A2	トラクター単体で駐車枠B手前に走行	PFMP
A3	駐車枠Bのトレーラーに接続	BIAGT
B1	トレーラーとともに駐車枠Bから走行経路に復帰	i-AGT
B2	トレーラーとともに駐車枠C手前に走行	PFMP
B3	駐車枠Cに駐車	i-AGT

3.2　経路生成管理機能

経路生成管理機能は，**図4**に示すように，自動運転タスク管理部と経路生成手法選択部，経路生成部から構成される。自動運転タスク管理部では，トラクターが実現すべき全自動運転タスクに関する情報，及び自身の位置情報を基に，トラクターが実現すべき自動運転タスクの順序と自動運転タスクごとの完了状態を定義する。それに加えて，現在タスクの完了状況に応じて，経路生成手法選択部へトラクターが取るべきタスクを指示する。経路生成手法選択部では，自動運転タ



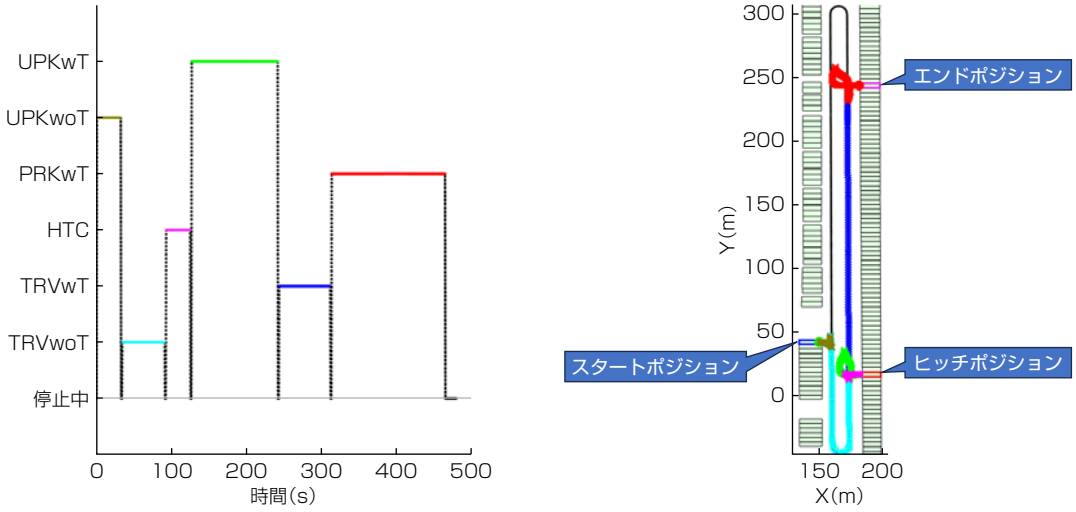
UPKwoT：Unparking maneuver without Trailer，TRVwoT：Traveling maneuver without Trailer，HTC：Hitching maneuver，
UPKwT：Unparking maneuver with Trailer，TRVwT：Traveling maneuver with Trailer，PRKwT：Parking maneuver with Trailer

図4-経路生成管理機能全体構成

スクに応じた経路生成手法を選択し，経路生成部は指示された経路生成手法を用いてタスクの完了状態に至るための経路を生成する。併せて，経路生成手法選択部では，トラクターがタスクの完了状態に至ると，自動運転タスク管理部に次のタスクを要求する。そして自動運転タスク管理部では，タスク完了に応じて次のタスクを経路生成手法選択部へ指示する。これらによって，トラクターの自動運転タスクと経路生成手法を適切に管理する。

3.3　検　　証

この手法を用いることで，機能要件を実現することを確認するために，閉ループシミュレーション環境での検証結果を示す。トラクターが自動運転タスクごとに経路生成手法を適切に切り替えて動作する様子を示すため，**図5**(b)ではトラクター位置に対して，**図5**(a)では時系列に対して，自動運転タスクごとに色分けした。検証の結果，スタートポジションからエンドポジションまでUPKwoT，TRVwoT，HTC，UPKwT，TRVwT，PRKwTの順にタスクを実現した。**図4**の自動運転タスク管理部のタスク順序と一致するとともに，途中停止やヒッチポジションを通り過ぎることもなかった。



(a)　自動運転タスク　　(b)　トラクター動作

図5－自動運転タスクの遷移とトラクター動作の結果

4. む　す　び

物流倉庫内のトレーラー自動搬送での，路側機の各種機能とトラクター側のセンサーフュージョン技術による認知，トラクターの経路生成手法について述べた。トラクターにセンサーを効率的に配置し，センサーフュージョン技術を活用したシミュレーションによってソフトウエア開発効率と開発速度を大幅に高めて，自動運転タスクに応じて複数の経路生成手法を適切に切り替えて管理する手法を開発した。このトレーラー自動搬送を社会実装することで，社会課題である労働力不足の解消に今後も取り組んでいく。

参 考 文 献

(1) Leu, J., et al.：Improved A－Search Guided Tree for Autonomous Trailer Planning, 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems, 7190～7196 (2022)
(2) Iqbal, H., et al.：Motion Planning of Articulated Vehicles with Active Trailer Steering by Particle Filtering, 2023 IEEE Conference on Control Technology and Applications, 478～483 (2023)
(3) Wang, Z., et al.：Motion Planning and Model Predictive Control for Automated Tractor－Trailer Hitching Maneuver, 2022 IEEE Conference on Control Technology and Applications, 676～682 (2022)

特集論文

グラフデータベースを用いたセキュリティープロトコル向け形式検証

Formal Verification Using Graph－Database for Security Protocols

毛利寿志*
Hisashi Mori
米持一樹†
Kazuki Yonemochi
三澤　学‡
Manabu Misawa

*三菱電機㈱ 情報技術総合研究所(博士(工学))
†同社 伊丹製作所
‡三菱電機デジタルイノベーション㈱

要　旨

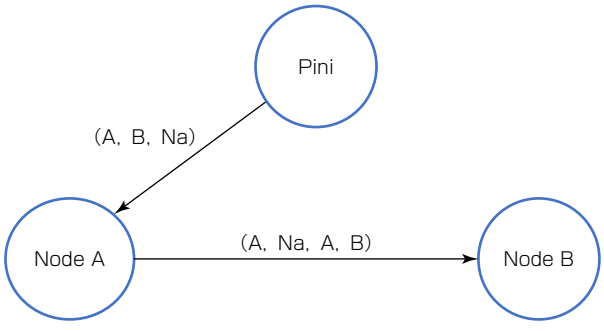
システム設計上，情報漏洩(ろうえい)や不正アクセス等の脆弱(ぜいじゃく)性が含まれないことを保証する方法として，セキュリティー検証がある。従来の検証方法では，形式言語理論やツール固有の言語といった高度な専門知識が必要，かつシステムが複雑になると検証が現実的な時間で完了しない，という課題があった。そこで，専門的で記述内容をすぐに理解しづらい言語表現ではなく，データ間の関係性を視覚的に把握できる一般的なグラフデータベース(以下“グラフDB”という。)を用いて，データ挿入と探索のデータベース操作でセキュリティー検証を可能にする方法を開発した。特定の暗号プロトコルを検証した結果，グラフ表示によって直感的な検証で従来と同様に脆弱性を検出した。さらに，検証時間が削減できることを理論的に示した。

1. ま え が き

システムの安全性やセキュリティーの確保に対する要求が高まっている。それらの確保には，設計段階でシステムが安全かつセキュアであると保証する方法が必要である。システムの一例としてセキュリティープロトコルがあるが，あるプロトコルが攻撃に対して正常に動作することを手動で解析することは困難である。この問題に対して，形式手法を用いた検証方法による解析の自動化は，有効な仕組みの一つと言える。セキュリティープロトコルに対する検証では，プロトコルやプロトコルに対する攻撃者の振る舞いを形式言語でモデル化し，プロトコルが満たすべきセキュリティー要求を検証項目として別の形式言語でモデル化し，ツールを用いて検証を実行する。このツールには，セキュリティープロトコル検証専用ツールと，汎用モデル検査器がある。このうちSPIN[(1)]等の汎用モデル検査器では，セキュリティーを含む様々な検証項目を記述できて，かつセキュリティーに関する検証事例も複数存在する。そのため，今回の研究ではセキュリティー検証の中でも汎用モデル検査器を用いた検証に焦点を当てる。様々なセキュリティープロトコルがSPINで検証されており，SPINを用いたセキュリティー検証の有用性は示されている。例えばMaggiらは，NSPK(Needham－Schroeder Public Key)プロトコルに対して検証を行い，脆弱性を導出した[(2)]。またHendaは，セキュリティープロトコル全般に対して盗聴や盗聴したメッセージの混入・再送を行う攻撃者を論理的に定義した。この定義を基に，NSPKプロトコルを含む３種類のセキュリティープロトコルに対して検証を行い，既知の脆弱性を導出した[(3)]。しかし，これらの従来技術は専用言語を習得する必要があるため，導入が比較的困難という課題があった。さらに，対象システムが複雑にな

```
mtype＝{A, B, Na};
Chan ca＝[0] of {mtype, mtype, mtype, mtype};
proctype Plni (mtype self; mtype party; mtype nonce)
{
        mtype g1;
        ca ! self, nonce, self, party;
}
proctype PRes (mtype self; mtype nonce)
{
mtype g2, g3;
        ca ? eval (self), g2, g3, eval(self);
}
init
{
        run Plni(A, B, Na)
}
```

(a)　従来技術SPINのプログラム記述例



(b)　グラフDBによる表示例

図１－従来技術SPIN及び提案手法グラフDBによる検証対象の表示例

ると，プロトコルや攻撃者の振る舞いを示す内部状態数が指数関数的に増大し検証が現実時間で完了しないという課題があった。

今回の研究では，最も広く利用されているグラフDBの一種であるNeo4j[4](注1)を採用し，グラフDBを用いたモデル検査を実装した。**図1**に，従来技術SPINによる対象システムの記述例と，同じ対象システムをグラフで表現したイメージ図を示す。**図1**は，送信者A(図中の$Node\ A$)が受信者B(図中の$Node\ B$)へ，メッセージNa及びAを受信者Bの公開鍵で暗号化し送信する通信(図中の$Node\ A$から$Node\ B$への矢印)を表す。

従来技術では，検証対象とするシステムの振る舞いを状態遷移に変換した後，その状態遷移をテキストでプログラムする(**図1**(a))。検証時にはプログラムが正しく検証対象を示していることを解読する必要がある。一方，提案手法によるグラフ表示ではシステムの振る舞いを視覚的に分かりやすく把握できる(**図1**(b))。ここで，$Pini$はプロトコルの開始を表す。また，矢印上の文字は，左から“送信者A，メッセージNa及びA，受信者Bの公開鍵で暗号化”を表す。対象システムを視覚的に分かりやすく把握できることによって，セキュリティー検証を行う際の負担を軽減できる。

(注1)　Neo4jは，Neo4j, Inc.の登録商標である。

2. 提案手法：グラフDBを用いたセキュリティー検証方法

直感的に検証できて，検証時間を削減できる，新たなセキュリティー検証方法を提案する。**2. 1節**では，セキュリティー検証方法として採用するモデル検査に必要な入力情報である対象システム，攻撃モデル，検証項目について，提案手法でどのように定義するかを述べる。**2. 2節**では，グラフDBを用いた実装方法及び実際に検証を実行した結果を述べる。

2. 1　提案手法の形式的表現の定義

提案手法では，検証したいセキュリティープロトコルや攻撃者の振る舞いを有向グラフで表して，検証したい性質をグラフDBのクエリーで表現することで，直感的な検証を実現している。この節では，グラフDB上で対象システム，攻撃モデル，検証項目をどのように定義するのかと，それらに対する検証結果が何を示すのかについて述べる。

(1)　対象システム

提案手法の対象システムは，既存モデル検査器の状態遷移と同等の有向グラフである。対象システムを有向グラフ(V, E)で表現する。ここで，Vは頂点の集合，Eは有向辺の集合である。次に，頂点と有向辺を定義する。

頂点は，r(送信者，受信者を示す項目)及びs(プロトコル中のどの状態かを示す項目)のラベルを含むと定義する。送信者(又は受信者)がプロトコルに沿ったメッセージを受信することを一つの頂点で表す。メッセージの内容が異なれば，それぞれ異なる頂点で表す。それらとは別に，プロトコル開始を表す$Init$及びプロトコル終了を表すEndの２種類の頂点を追加する。

有向辺は，t(暗号文又は平文を示す項目)，m(送信されるメッセージ内容を示す項目)，k(メッセージを暗号化する鍵を示す項目)のラベルを含むと定義する。プロトコル送信元から受信先までを一つの有向辺とする。

(2)　攻撃モデル

セキュリティープロトコルの脆弱性を網羅的に検査できる攻撃モデルとしてDolev-Yaoモデルが著名であり，**1章**で述べたHendaの研究[3]でも採用されている。提案手法でも同様に，Dolev-Yaoモデルに基づくHendaの攻撃モデルを用いる。すなわち，Hendaの攻撃モデルを追加した対象システムに対して，セキュリティー要件を満たすか否かを検証する。紙面の都合上，Hendaの攻撃モデルの厳密な定義については原著論文[3]を参照されたい。

攻撃モデルを対象システムに追加する手順を示す。まず，事前準備として，攻撃者が知る情報の集合$\mathbb{K}$を$ACTOR$(送信者／受信者／攻撃者)，$PLAIN$(平文)，$CIPHER$(暗号文)，$PKEY$(公開鍵)，$SKEY$(秘密鍵)の部分集合に分割する。ある状態を送信元とした場合の攻撃を表す頂点及び有向辺の作成手順は次のとおりである。

①$ACTOR$，$PLAIN$，$PKEY$の中から各要素を選択し，全ての組合せについて暗号文を作成

②送信する先の頂点(送信者又は受信者)が存在しない場合，送信先の頂点を作成

③作成した各暗号文又は$CIPHER$に格納済みの各暗号文をラベルとして，送信元-送信先の有向辺を作成

(3)　検証項目

提案手法では，従来技術SPINと同様に，検証項目として形式言語の一種であるLTL(Linear Temporal Logic：線形時相論理)相当の記述[5]を想定する。検証項目の一例として，ユーザー認証を取り上げる。従来技術[2][3]によると，モデ

ル検査でのユーザー認証(送信者Aが確かに受信者Bを認証している)の定義は,“送信者Aがプロトコルを実行完了したときはいつでも,他者Bはプロトコルを実行している”である。

⑷　検証結果

対象システム及び攻撃モデルを表す有向グラフ上で検証項目を表すクエリーを実行し,クエリーを満たさない経路が出力された場合,その検証項目が満たされなかったことになる。先に述べたとおり,提案手法の有向グラフとクエリーは,それぞれ従来技術(モデル検査器)の状態遷移と検査項目と同等である。したがって,クエリーの出力は従来技術の検証結果と同等である。

2.2　グラフDBを用いたモデル検査の作業フロー

この節では,提案手法であるグラフDBを用いたモデル検査の作業フローについて述べる(**図2**)。

⒜　従来技術　　⒝　提案手法

図2-従来技術及び提案手法を用いたセキュリティー検証の作業フロー

従来技術(**図2**(a))では,検証したいシステム仕様や攻撃モデルを選択した後,形式言語へ手動変換し,さらにモデル検査器のプログラムに変換してからモデル検査器で検証実行する必要があった。一方,提案手法(**図2**(b))では,検証したいシステム仕様と攻撃モデルを選択し,検証を実行するだけで検証結果が得られる。提案手法は,任意のセキュリティープロトコルについて,プロトコルや攻撃モデルをグラフDBに変換するアルゴリズムである。アルゴリズムを確立すれば,変換の自動化は容易であるため,今後プロトコルや攻撃モデルのグラフDBへの変換を自動化することを予定している。モデル検査手法にグラフDBを用いることで,設計者は一般のDB操作である頂点や有向辺の追加及び経路探索の知識でモデル検査の実施が可能になる。また,グラフDBを用いたことや,攻撃者の状態数,プロトコルで送受信される情報を表す変数,及び偽メッセージを適切に削減したことによって,提案手法を用いた検証は,従来技術に比べて,検証に必要な内部状態数を削減できる。

グラフDB上での実装の例題として,**1章**で挙げたNSPKプロトコルを対象に,**2.1節**で述べた検証項目である認証について検証した。具体的には,NSPKプロトコルや攻撃モデル,認証を表す論理式を**2.1節**で示した手順に沿ってグラフDB上で表現し,認証を満たさない経路のうち最短経路を求める方法と,全経路を求める方法を実行した。ここで,検証対象及び検証項目について検証を実行した際,その検証項目を満たさない経路が出力される。一方,検証対象が検証項目を満たす場合は,何も出力されない。実行した結果,両方の方法でそれぞれ反例が出力された。2種類の経路について検証項目を満たさないことを目視で確認したことによって,検証結果が正しいことを確認した。なお,紙面の都合上,NSPKプロトコルを表すグラフや検証結果のグラフは省略する。

3.　評　　価

従来技術であるSPINを用いた検証方法も,提案手法によるグラフDBを用いた検証方法も,対象システムの振る舞いを状態遷移として表して,検証項目を満たさない状態に到達した場合は反例として出力する。すなわち,検証時間は,作成される状態数に依存する。状態が多すぎる場合は検証が現実的な時間で完了しない危険性がある。そこでこの章では,

実行時間に関する論理的な評価として，従来技術及び提案手法で作成される状態数を比較する。状態数を比較した結果，提案手法は従来技術に比べて常に少ない状態数であることを確認した。例えば，NSPKプロトコル（メッセージ数$m=3$）の場合，従来技術の状態数は15,275である一方，提案手法は状態数20であり，約763分の１である（**図３**）。従来技術SPINでの状態数は，対象システムの状態数と検証項目の状態数の積で表される。一方で提案手法の状態数は，対象システムの状態数だけである。これは，グラフDBの探索機能によって，対象システムの状態だけを探索することで検証できるためである。従来技術及び提案手法の状態数をそれぞれ算出し，比較した結果を次に示す。

従来技術であるHendaの方式では，状態数は次の式で表される。

$$\{m+3+\sum_{i=0}^{m}\{(|Knows|-|PKEY|)^{(t-t_{|PKEY|}+(i-1))} \times\{(|Knows|-|PKEY|)^{(t-t_{PKEY})}\times|PKEY|+1\}\}\} \times(2^{|TL|}+1)$$

ここで，mはメッセージ数，$|Knows|$は攻撃者が知る情報の要素数，$|PKEY|$は攻撃者が知る情報のうち公開鍵の要素数，tは１メッセージ当たりの項数，$t_{|PKEY|}$は１メッセージ当たりの公開鍵を表す項数，$|TL|$は検証項目の各部分式の一番外側の演算子が様相演算子である式の集合をTLとしたときのTLの要素数である。

一方，提案手法では，状態数は次の式で表される。

$$(m+3)+|Init|+\sum_{i=0}^{m}((|PLAIN|^{t_{PLAIN}}+i+1))$$

ここで，$|Init|$は最初の送信者の状態数，$|PLAIN|$は平文全体の要素数，t_{PLAIN}は１メッセージ当たりの平文を表す項数である。

このような式に基づいて，Hendaの方式と提案手法についてメッセージ数mに伴う状態数の変化を比較したグラフを**図３**に示す。全体を通して，提案手法の方が従来技術よりも少ない状態数になることが分かる。一般のパソコンでは状態数500,000程度が検証の限界と言われている[6]。従来技術ではメッセージ数７のとき状態数が500,000を超えるが，提案手法では状態数が62と抑えられたままである。

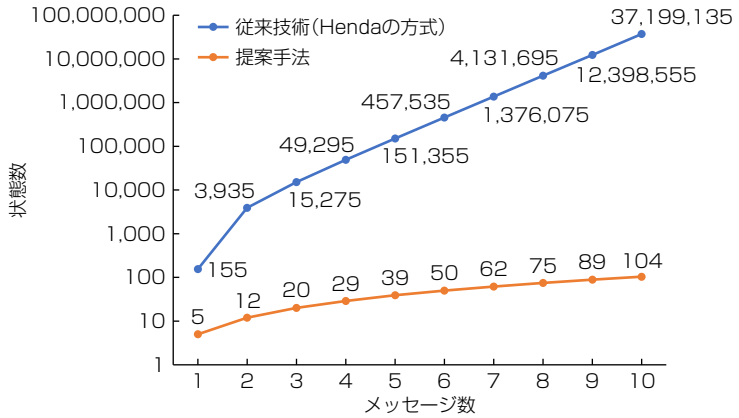


図３−メッセージ数に伴う従来技術及び提案手法の状態数の変化

4. む　す　び

セキュリティープロトコルを例題に，対象システムをグラフDBの有向グラフで記述し，検証項目をグラフDBのクエリーで記述するモデル検査手法を提案した。グラフDBという一般的な知識でグラフを作成できて，グラフを可視化する機能によって直感的な理解が可能になる。また，グラフDBの全パス探索機能を用いて，全反例を出力するモデル検査の実行も可能になる。さらに，有向グラフに対して検証項目を直接クエリーで記述し探索することで，モデル検査実行に際して状態数を削減できて，自動での検証が現実的な時間で可能になる。

今後，ほかのセキュリティープロトコルを対象にした場合に，従来技術SPINと提案手法で実行結果や状態数にどの程

度違いがあるかを検証する予定である。さらに，提案手法が認証以外の性質も定義・検証できることを示す予定である。また，システムの安全性も含めた検証を行えるよう，対象システムや検証項目の形式化を拡張する予定である。今後，システムはますます複雑になり，セキュリティー機能が正しく搭載されていることを手動で判断することが困難になる。提案手法を用いてシステムのセキュリティーを自動で保証することによって，設計段階の工数を大幅に削減できる。

参 考 文 献

(1) Holzmann, G. J.：The SPIN Model Checker，Addison－Wesley (2004)
(2) Maggi, P., et al.：Using SPIN to Verify Security Properties of Cryptographic Protocols，Lecture Notes in Computer Science，**2318**，187～204 (2002)
(3) Henda, B. N.：Generic and Efficient Attacker Models in SPIN，Proceedings of the 2014 International SPIN Symposium on Model Checking of Software，77～86 (2014)
(4) Robinson, I，ほか：グラフデータベース－Neo4jによるグラフデータモデルとグラフデータベース入門，オライリー・ジャパン (2015)
(5) 久野和敏，ほか：グラフデータベースを用いたモデル検査手法の提案，第198回SE研究発表会 (2018)
(6) Joesang, A：Security Protocol Verification using SPIN，the First SPIN Workshop(SPIN’95) (1995)

特集論文

おとりを用いた内部犯検知技術

Insider Threat Detection Using Decoy

山本　匠*
Takumi Yamamoto
野澤康平†
Kohei Nozawa
宇谷亮太†
Ryota Udani

*情報技術総合研究所（博士（情報学））
†同研究所

要　旨

サイバー攻撃による情報漏えいが課題であると言われているが，実際には，内部犯による情報漏えいも数多く発生している(1)。内部犯は正規の権限を持つ悪意を持ったユーザーであり，既存のセキュリティー対策ではその兆候を明確に捉えることが難しい。内部犯の悪意を顕在化させるために，囮（おとり）に着目した。普段とは異なる活動をするユーザーに対して，動的に囮のファイルを配置し，囮のファイルへのアクセスの傾向を基に内部犯を絞り込む手法を開発した。

1．ま え が き

“内部不正による情報漏えい等の被害”はIPA（独立行政法人 情報処理推進機構）が公開する“情報セキュリティ10大脅威2025”で第４位であり，10年連続で10大脅威として取り扱われている(2)。また重要インフラや工場などのOT（Operational Technology）環境でも，内部犯による不正は，深刻な脅威として認識されている(3)。このことからも内部犯への対策の検討が必要と言える。本稿では，三菱電機の内部犯に対する技術的な対策の取組みについて述べる。

2．内部犯の脅威

本稿で扱う内部犯の定義は，正規のアカウントを持つ悪意を持ったユーザーである。内部犯に対しては，一度認証されたユーザーを原則信用する，従来の監視・防御モデルでの対策は難しい。そのため，あらかじめ分析しておいたユーザーの正常な振る舞いから，振る舞いの異常をリスク値として評価し高リスクのユーザーをあぶり出す，アノマリー検知やUEBA（User and Entity Behavior Analytics）などの振る舞い分析技術の適用が有効であると考えられている(4)。しかし，ユーザーの業務内容は多岐にわたり，また，同一ユーザーが同じ業務を行うときでもユーザーの振る舞いは変動するため，正確にリスク値を算出することは難しい。また内部犯は見つからないように振る舞い分析技術が低リスクと評価する範囲で不正を働くことが考えられ（例えば，少しずつ機密ファイルをアップロードする），振る舞い分析技術で厳しく監視すれば誤報が頻出してしまう。

これらのことから，内部犯を正確に見つけだすことは非常に難しい課題であると言える。正規の権限の範囲で悪意のある行為を実行するという性質上，内部犯と悪意のないユーザー（“正規ユーザー”という。）との差は，悪意の有無だけであり，振る舞いを受動的に観測しているだけでは識別が困難である。

3．提案する内部犯対策技術

そこで筆者らは，受動的に観測できる情報だけから内部犯と正規ユーザーとを切り分けるのではなく，内部犯なら積極的に行うであろう行為を防御側が能動的に誘発させることで，内部犯の悪意を間接的に顕在化させ，悪意に関連する行為を観測するというアプローチを採用した。内部犯の悪意を間接的に顕在化させるために，普段とは異なる活動をするユーザーに対して，もしそのユーザーが内部犯であれば興味を引きそうな囮ファイルを動的に配置し，囮ファイルへのアクセスの傾向を基に内部犯を絞り込むというのが，提案方式のコンセプトである。

提案方式の概要は次のとおりである（**図１**）。

①アノマリー検知などの振る舞い分析システムでファイルアクセスのログなどを分析し，振る舞いの異常をリスク値として算出する。さらに，対象ユーザー名，リスク値，ファイルアクセスの情報を含むリスク情報を作成する。

②囮システムは，振る舞い分析システムからリスク情報を受け取って，高リスクのユーザーに対しては，そのユーザーが興味を引きそうなトピックをファイルアクセスの情報から推定し，そのトピックに関連するコンテンツを含んだ囮ファイルを，様々なトピックの囮ファイルが保存された囮データベースの中から選択する。その後，選択された囮ファイルが，あたかもファイルサーバー上に配置されているかのように当該ユーザーのファイルエクスプローラーの表示を制御する。内部犯にとって魅力的な囮ファイルを配置することで，囮ファイルを選択する確率が増えて，内部犯をより特定しやすくする。配置した囮ファイルに関する情報(ファイル名，対象ユーザー名など)は囮情報として振る舞い分析システムへと渡される。

③振る舞い分析システムは，通常のファイルと同様に，囮ファイルへのアクセスも監視する。振る舞い分析システムは，囮システムからの囮情報を基に，囮ファイルへのアクセスの有無を判断する。囮ファイルへのアクセスがあれば，振る舞い分析システムのリスク値(又はしきい値)にフィードバックすることで，囮ファイルに積極的にアクセスするより高リスクなユーザーに対する監視を強化し，内部犯の候補として絞り込んでいく。

高リスクと判定されたユーザーに絞って囮ファイルを配置することで，普段どおりの業務をしている低リスクの正規ユーザーへの業務阻害を軽減できる。万が一正規ユーザーが高リスクと判定され，囮ファイルが配置されたとしても，普段使っているファイル以外へは積極的にアクセスすることはないと考えられ，業務阻害の可能性は低いと期待する。

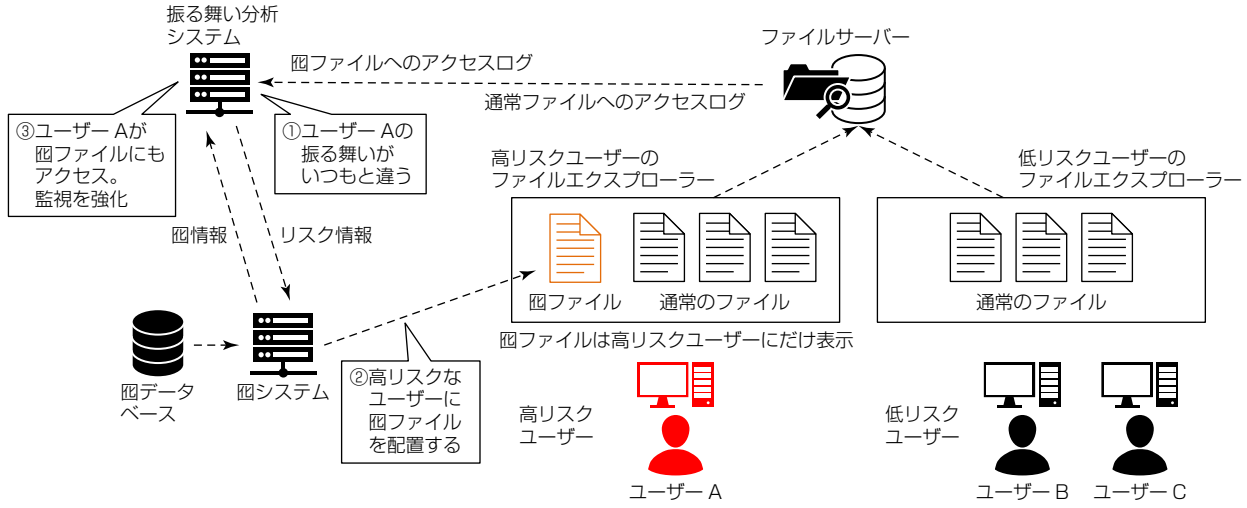


図１−提案方式の概要

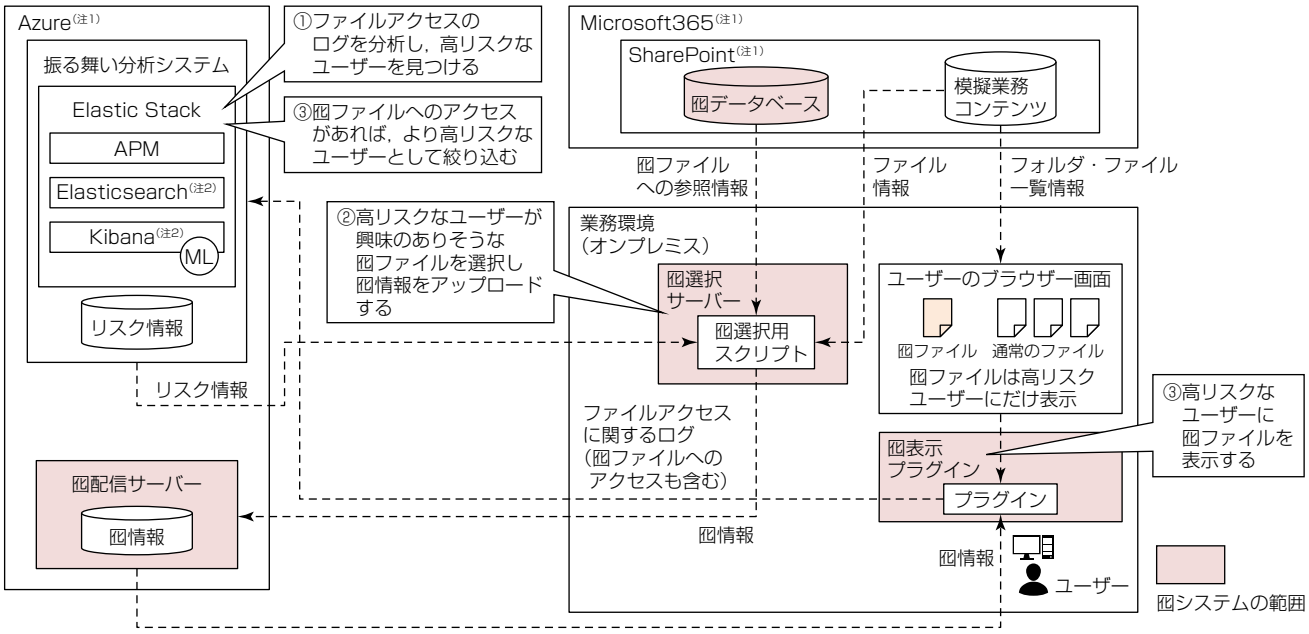
4. 提案方式の試作と動作イメージ

提案方式の実現性の確認のため，試作を行った。試作したシステムの構成を**図２**に示す。

詳細については筆者らの既存研究[5]を参照されたいが，**図２**の囮選択サーバー，囮配信サーバー，囮表示プラグイン，及び囮データベースが連携し，**図１**の囮システムに該当する機能が実現される。昨今のクラウドベースのファイルのやり取りの増加から，今回の試作では**図１**に示すファイルサーバーは利用せず，代わりにSharePoint[6]上に業務で使うファイルを模擬したコンテンツを配置した。振る舞い分析システムはAzure[7]上にElastic Stack[8]を用いて構築した。囮配信サーバーもAzure上に構築した。囮データベースから囮ファイルの参照情報を取得する囮選択サーバーは，業務環境上に構築した。囮データベースは，模擬業務コンテンツと同じSharePoint上に配置した。SharePoint上のファイルにブラウザーでアクセスすることを想定し，対象ユーザーにだけ囮ファイルを閲覧可能にするための制御は，ブラウザーに囮表示プラグインを導入することで実現した。

4.1　試作システムの動作の流れ

次にシステム構成上の動作の流れを述べる(**図２**)。



APM：Application Performance Monitoring，ML：Machine Learning
（注１） Azure，Microsoft365，SharePointは，Microsoft Corp.の登録商標である。
（注２） Elasticsearch，Kibanaは，Elasticsearch B.V.の登録商標である。

図２−試作したシステムの構成

①振る舞い分析システムは，SharePointのファイルアクセスに関するログを分析し，リスク値を算出する。さらに，高リスクのユーザーの名前，リスク値，高リスクと判断されたファイルアクセスの情報を含むリスク情報を作成する。

②囧選択サーバーは，リスク情報を振る舞い分析システムから定期的に取得し，高リスクのユーザーが直近にアクセスしたファイルの情報(ファイル名やファイルのコンテンツなど)からファイルのトピックを推定する。囧データベースからトピックに関連する囧ファイルへの参照情報を取得後，当該ユーザー向けの囧情報を作成し，囧配信サーバーにアップロードする。

③囧表示プラグインは，定期的に囧配信サーバーから囧情報を取得し，高リスクなユーザーであれば囧ファイルを表示する。今回の実装では，囧システムから振る舞い分析システムに送られる囧情報(**図１**)の代わりに，囧表示プラグインから振る舞い分析システムに対して，SharePoint上のファイルへのアクセスのログと一緒に囧ファイルへのアクセスかどうかの情報(ラベル)も送信している。振る舞い分析システムが囧ファイルへのアクセスを確認した場合，当該ユーザーをより高リスクなユーザーとして絞り込む。

4.2　試作システムの動作イメージ

振る舞い分析のリスク値のダッシュボードや囧ファイルが表示される画面を例に，試作物の動作イメージを述べる(**図３**)。

①振る舞い分析システムが，ユーザーのSharePointのファイルアクセスに関するログを分析し，リスク値を算出する。リスク値をダッシュボードに可視化した例を**図３**に示す。グラフ横軸は時刻，縦軸がリスク値であり，折れ線が各時刻での，あるユーザーの振る舞いに対するリスク値の算出結果を示している。

②振る舞い分析システムは，リスク値が所定のしきい値を超えた場合にアラートを発報し，リスク情報を作成する。囧選択サーバーは，リスク情報を取得することでアラートの有無を確認する。通常時，しきい値はθ_1に設定されている(**図３**のピンクの線)。**図３**の例では，②の時点で，リスク値がしきい値θ_1を超えたため，この直後にリスク情報が作成され囧選択サーバーがアラートを確認する。アラートにはリスク値のほかに，しきい値やアクセスしたファイルの情報などが付与される(**図３**中のダッシュボード下部)。

③アラートが発報されると，当該ユーザーには囧ファイルが表示される。囧データベースから得た情報を基に囧ファイルのメタ情報(タイムスタンプ，ファイルサイズ，更新者など)も再現可能である。ブラウザーで囧ファイルを表示した例を**図４**に示す。**図４**(a)の例では，説明の都合上，囧ファイルかどうかが分かるように，“**【囧】**”という文字列をファイル名に付与している。**図４**(b)の例では，囧ファイルをブラウザーで開いたときの画面である。なお本稿の図の

中に示されているファイル名やファイルのコンテンツは，実際の業務とは一切関係のない架空のものである。また囮ファイルの用意については今回手作業で行ったが，昨今急速に進化している生成AI技術を活用すれば，品質の高いコンテンツの囮ファイルを大量に自動生成することも可能であると考えるが，生成されたコンテンツの著作権については十分注意が必要である。

④ユーザーが囮ファイルにアクセスしたら，アラート発報のしきい値を，当該ユーザーだけ厳しい値に変更($\theta_1 \rightarrow \theta_2$)し，監視を強める。**図３**の例では，利用するしきい値がピンク色の線(θ_1)から緑色の線(θ_2)に変わって，低いリスク値でもアラートが発報されるようになる(**図３**の④)。囮ファイルへのアクセスが一定期間なければ，しきい値は元の値(θ_1)に戻す。囮ファイルへのアクセスの有無が分かるように，囮ファイルへのアクセスがあった場合，青色の折れ線グラフを，リスク値の折れ線グラフに加えた形で描画している(**図３**の③)。囮ファイルか否かについては，ファイルアクセスログに付与されるラベルを基に判断する。

なお，説明の都合上，**図３**のリスク値は，あらかじめ決めたルールに基づいて算出されている。実運用ではあらかじめ手作業でルールを定義する必要のない機械学習によるアノマリー検知技術を使うことも可能である。

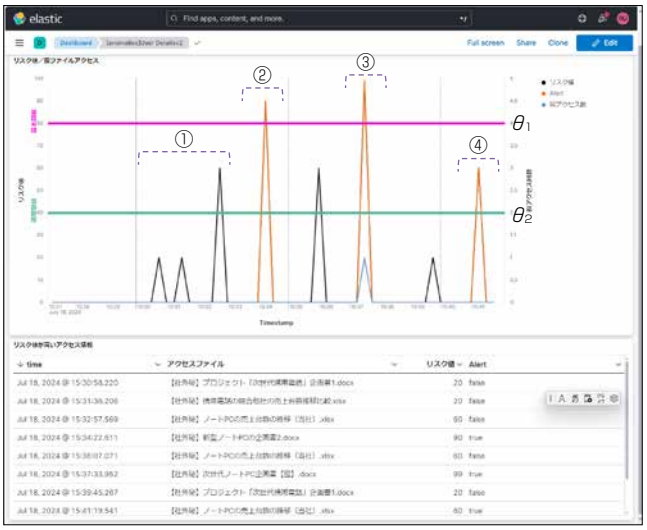


図３−振る舞い分析のリスク値のダッシュボードの例

(a)　SharePoint画面上に表示される囮ファイル

(b)　囮ファイルをブラウザーで開いたときの画面

図４−囮ファイルを表示した例

4.3　対策を無効化する可能性への対応

最後に，この対策の導入を知った内部犯が対策を無効化する可能性が考えられる。プラグインを無効化する攻撃については，プラグインの導入を組織のグループポリシーで強制し，機密ファイルが置かれたSharePointにプラグインなしではアクセスできない環境にすることで対策可能である。ファイルのメタ情報や囮情報などを確認し囮ファイルを見分けようとする内部犯に対しては，当該行動を危険な振る舞いとしてスコアリングし，相補的な監視をすることで対策可能である。

5. む　す　び

従来の方法では検知が困難であった内部犯の脅威に対して，内部犯の悪意を間接的に顕在化させるために，普段とは異なる活動をするユーザーに動的に興味を引きそうな囮ファイルを配置し，囮ファイルへのアクセスの傾向を基に内部犯を絞り込む手法を提案した。また簡単な実装例を示し，実現可能性を示した。

今後は，過去の内部犯の事例などを基にユーザースタディーを行い，提案方式の有効性の考察を行っていく。

参 考 文 献

(1) Proofpoint, Inc.：2022 COST OF INSIDER THREATS GLOBAL REPORT（2022）
https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf

(2) 独立行政法人 情報処理推進機構：情報セキュリティ10大脅威 2025（2025）
https://www.ipa.go.jp/security/10threats/10threats2025.html

(3) National Counterintelligence and Security Center：INSIDER THREAT MITIGATION FOR U.S. CRITICAL INFRASTRUCTURE ENTITIES, GUIDELINES FROM AN INTELLIGENCE PERSPECTIVE（2024）
https://www.dni.gov/files/NCSC/documents/nittf/20240926_Insider-Threat-Mitigation-for-US-Critical-Infrastructure.pdf

(4) 日本アイ・ビー・エム㈱：ユーザーおよびエンティティーの行動分析（UEBA）とは
https://www.ibm.com/jp-ja/topics/ueba

(5) 山本　匠，ほか：おとりを用いた内部犯検知システムの提案，コンピュータセキュリティシンポジウム2024論文集，494～500（2024）

(6) Microsoft Corp.：What is SharePoint?
https://support.microsoft.com/en-us/office/what-is-SharePoint-97b915e6-651b-43b2-827d-fb25777f446f

(7) Microsoft Corp.：What is Azure?
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure

(8) Elasticsearch B.V.：Elastic Stack
https://www.elastic.co/jp/elastic-stack

三菱電機株式会社