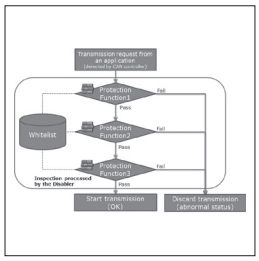


Controller Area Network (CAN) の不正送信防止機構の提案

A Proposal of the Device Disabler for Controller Area Network

上田　浩史* Hiroshi Ueda
倉地　亮* Ryo Kurachi
本田　晋也 Shinya Honda
高田　広章 Hiroaki Takada
足立　直樹 Naoki Adachi
宮下　之宏 Yukihiro Miyashita

車載制御ネットワークではController Area Network（CAN）が広く使用されており、現在販売される車両に搭載される電子制御ユニットにはセキュリティ上の強化策が十分に搭載されていない。しかしながら、この10年の間にCANに対する多数のセキュリティ脅威事例が報告されている。このため、本稿では、適切ではないメッセージの送信を拒否するように改造された通信コントローラを用いることにより、CANやCAN FDバス上への不正な送信を防止する手法について提案する。

Recently, quite a number of security attacks against Controller Area Networks (CAN) have been reported. Many automotive companies are planning to adopt security countermeasures to strengthen security of their in-vehicle systems while saving the costs. This paper proposes a method to block unauthorized CAN-bus access using our enhanced CAN controller that prevents the transmission of messages from a malicious electronic control unit. We also demonstrate the effectiveness of our device disabler on a CAN with Flexible Date rate buses.

キーワード：車載制御ネットワーク、セキュリティ、Controller Area Network（CAN）、CAN FD

1. 緒　　言

現在の自動車は、電子制御ユニット（Electronic Control Unit：ECU）と呼ばれる小型のコンピュータが多数搭載されており[(1)]、これらECU同士が車載制御ネットワークを介して情報を交換することで、車の制御を実現している。この電子制御システムで広く使用される通信プロトコルとして、Controller Area Network（CAN）[(2)]が存在し、その後継プロトコルであるCAN with Flexible Data rate（CAN FD）も広く普及することが予想されている。その一方で、近年、車載制御ネットワークを利用したサイバー攻撃事例が多数報告されている。

Koscherらは、偽造されたCANメッセージを車載制御ネットワークに送信することにより、自動車の制御を乗っ取れることを実証した[(3)]。Valasekらは、不正な機器をCANバス上に配置することで、容易に不正送信できることを実証した[(4)]。また、Millerらの最近の研究では、携帯電話網を経由し、CANバス上に接続されているECUのプログラムを書き換え、不正送信が実現できることを示した[(5)]。このように、ECUのプログラムを書き換えることにより、不正なCANメッセージを送信し、制御を乗っ取る攻撃事例が多数指摘されている。

そこで、本稿では、これらの攻撃の対策手法としてCANメッセージの不正送信防止機構を提案する。より具体的には、改良されたCANコントローラに不正送信防止用の監視機構を実装することにより、プログラムを書き換えられたり、マルウェア※1を注入されたECUによる不正なCANメッセージの送信を防止する手法を提案する。

2. CANの特徴

CANは、ISO11898で標準化された通信プロトコルであり、以下の特徴を持つ。

(a) バストポロジ

1つの通信線に複数のノードが接続されるバストポロジで広く使用されている。

(b) 送信権の調停

各ノードは送信したいメッセージが発生するとすぐに送信動作に移行するマルチマスタ方式を採用するため、複数のノードが同時にCANバス上へとメッセージを送信すると、メッセージの衝突が発生する。これを解決するために、CAN-IDを用いた送信権の調停が実施される。この結果、最も優先度の高いメッセージを持つCANメッセージが優先的に送信される。一方、優先度の低いメッセージはより高い優先度のすべてのメッセージの送信が完了するまで送信開始が遅延する。

(c) メールボックス

CANの通信コントローラでは、メッセージを送受信するためのレジスタ群をメールボックスと呼ぶ。一般的なCANコントローラでは、様々なシステムに適用できるよう送信メールボックスと受信メールボックスが複数搭載されてい

ることが多い。このため、各ノードはCANコントローラが用意する送信用あるいは受信用メールボックスを複数使用するが、必ずしもすべてのメールボックスを使用しているとは限らない。

3. 不正送信防止機構の提案

本章では、提案手法であるCANの不正送信防止機構を説明したうえで、既存の攻撃事例に対して提案手法が有効であることを説明する。

3−1 不正送信防止機構

脅威として、文献 (5) と同様の手段により、外部ネットワークを通じてECUのプログラムが攻撃者により不正に書き換えらえる攻撃が想定される。本提案手法では、このプログラムを書き換えられたECU（以降、踏み台ECUと呼ぶ）のCANバスへの利用制限を行うことにより、踏み台ECUによる車載制御システムへの攻撃を最小限に留めることを目的とする。なお、不正送信防止機構が提供する保護機能は、以下のとおりである。

(a) 保護機能1：未使用メールボックスの利用制限
設計上、各ECUが送受信のために使用するメールボックスを制限することで、もし踏み台ECUとなった場合でも未使用であるメールボックスの悪用を抑止できる。

(b) 保護機能2：ホワイトリスト[※2]による送信可能メッセージの制限
各ECUが送信すべきCANメッセージは設計時に決定される。このため、各ECUから送信できるCANメッセージを予め制限することで、もし踏み台ECUとなった場合でも、それ以外のメッセージの送信を抑止できる。

(c) 保護機能3：異常な送信頻度による送信
各ECUが送信すべきCANメッセージの送信頻度は設計時に決定される。このため、もし踏み台ECUとなった場合でも本来送信すべきCANメッセージの送信頻度を超えてCANメッセージを送信することを抑止する機構を持つ。

現状のECUでは、これらの保護機能が実装されていないために、プログラムが不正に書き換えられたりマルウェアが注入されると容易に踏み台ECUからの不正送信が可能となる。より具体的には、以下の脅威が存在する。

保護機能1が未実装の場合、マルウェアが踏み台ECUの正規アプリケーションになりすまし、未使用のメールボックスを利用して不正なCANメッセージを送信することが可能となる。保護機能2が未実装の場合、マルウェアが踏み台ECU以外の正規ECUになりすまし、不正なCANメッセージを送信することが可能となる。保護機能3が未実装の場合には、踏み台ECUが異常な頻度でメッセージを送信することによりCANバスへのDoS攻撃[※3]が可能となる。

3−2 実現方法

提案手法は、既存するCANコントローラのハードウェアを拡張することにより実現する。不正送信防止機構とは、CANメッセージの送信要求時に送信可能なメッセージかどうかを判断するよう実装されたハードウェアのことである。送信可能なCANメッセージの情報（CAN-ID、DLCなど）とその送信周期および使用可能な送信メールボックスのIDなどの情報は、CANコントローラ内の不正送信防止機構にホワイトリストとして設定されている必要がある。

そのうえで、**図1**の検査手順を用いて、以下の検査1から検査3を実施することにより、送信要求されたメッセージの送信可否を判定する。

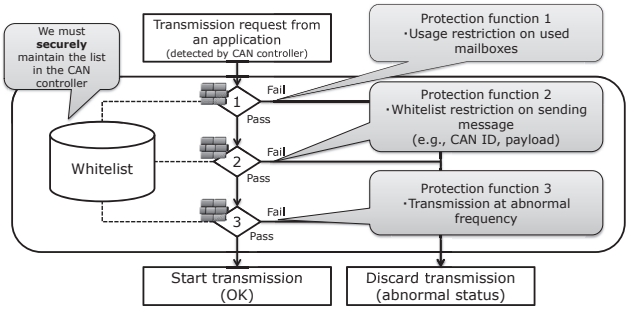


図1 送信要求処理時の検査手順

(a) 検査1：送信に使用できるメールボックスかどうかを検査する。このとき、送信に使用できないメールボックスを使用し送信しようとしている場合には送信を破棄するものとし、送信可能なメールボックスを使用する場合には送信動作を継続し検査2を実施する。

(b) 検査2：送信可能なCANメッセージかどうかをホワイトリストから検査する。もし送信が許可されないCAN-IDのメッセージを送信しようとする場合にはこの送信を破棄する。一方で送信可能な場合には送信動作を継続し検査3を実施する。

(c) 検査3：送信要求の送信周期を検査する。もし予め設定された送信周期を上回る頻度で送信要求がある場合には、この送信を破棄する。一方で送信頻度が低い場合には、この送信を許可する。

3−3 ホワイトリストの書き込み方法

本提案手法では、ホワイトリストが改ざんされるようであれば監視機構が無力となるため、ホワイトリストの保護が重要となる。このため、以下の2つの手順のいずれかによりホワイトリストを書き込むことを想定する。なお、ランタイム上でホワイトリストを書き込む場合には、ホワイトリストが1度設定された後、これを書き換えられないように保護する必要がある。このため、本稿で提案する不正

送信防止機構では、次に示す書き込み方法2が使用される場合には、リセット解除後、ホワイトリスト書き換え完了レジスタが設定されるまでの期間はホワイトリストを設定できないようにする必要がある。

(a) **書き込み方法1：認証された専用ツールから書き換え可能なフラッシュROMに出荷時に書き込む。**現在、市販されているマイコンの中には、このような手段を用いて、マイコンへ供給されるクロックの設定などが行われることがあるため、これと同様の機構を用いることを想定する。

(b) **書き込み方法2：セキュアブートを使用し、不正送信防止機構にホワイトリストを設定する。**この場合には、セキュアエレメントなどを用いて、セキュアブートを実行する必要があるため、既存するECUよりも追加のハードウェアコストが増加する恐れがある。

現状では、すべてのECUでセキュアブートを実施しているわけではないため、書き込み方法1が既存する車載制御システムに親和性が高く、コスト効率が高い方法と考えられる。

3−4　想定するユースケース

metromile[6]などのサービスを利用するには、各自動車にOBD-IIドングルと呼ばれる診断用通信機器を取り付ける必要がある。これらのドングルは、走行距離に応じて保険料を割り引く目的で取り付けられており、CANネットワーク上に送信される走行距離関連の情報をサービス会社のサーバーへアップロードする。しかしながら、使用されるOBD-IIドングルの脆弱性を悪用して、攻撃者のサーバーから不正なプログラムをダウンロードさせることにより、CANバス上に不正なメッセージを流すという攻撃事例がある。

もしこのOBD-IIドングルに本稿で提案する不正送信防止機構が搭載されていた場合、CANバス上への送信メールボックスはないものとして不正送信防止機構に設定しておけば、前述する（検査2）により、不正なCANメッセージの送信を防ぐことが可能になる。

また、Millerらが発表したECUに対するプログラムの改ざん事例[5]についても、プログラムが書き換えられた踏み台ECUが本来送信するメッセージの送信を許してしまうものの、他のECUから送信されるメッセージのなりすましに関しては抑止することが可能である。これらの結果より、本稿で提案する不正送信防止機構により、不正なメッセージの送信をハードウェアで抑止することは非常に有用性が高いと考えられる。

4.　不正送信防止機構の実装

我々の提案する不正送信防止機構を、アルテラ社のFPGAボード上へ実装した（**図2**）。

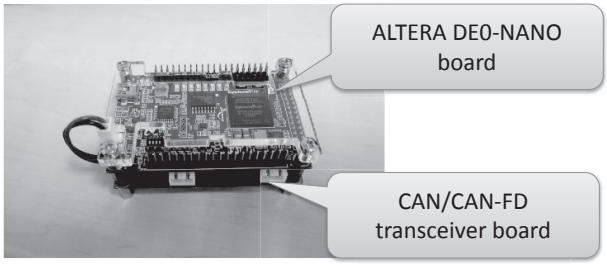


図2　実機評価環境

4−1　最低送信周期カウンタの実装

最低送信周期カウンタは、CANコントローラ上で生成されるCANネットワーク上の1ビット時間単位のカウンタとして実装した。本カウンタの起動は、初回送信要求が発生した後にカウントアップが開始され、以降は監視が開始されるものである。このため、初回送信要求時については、最低送信周期カウンタによる保護はなされないものの、2回目以降の送信要求時には、その頻度が設定された最低送信周期が守られていない場合、CANバス上への送信は行われず、CANコントローラ上で送信要求が破棄される構成とした。

4−2　不正送信防止機構の実装

不正送信防止機構は既存するCANコントローラIPの中のサブモジュールとして埋め込むように実装した（**図3**）。本システム全体は、Nios IIソフトコアと改造されたCANコントローラの他に、DRAMコントローラ、オンチップRAMなどを実装した。本システムの合成結果については、23,888ロジックエレメントを消費しており、CANコントローラで5,374ロジックエレメントを使用した。なお、既存するCANコントローラIPを用いて合成するよりも、3,106ロジックエレメント増加した。

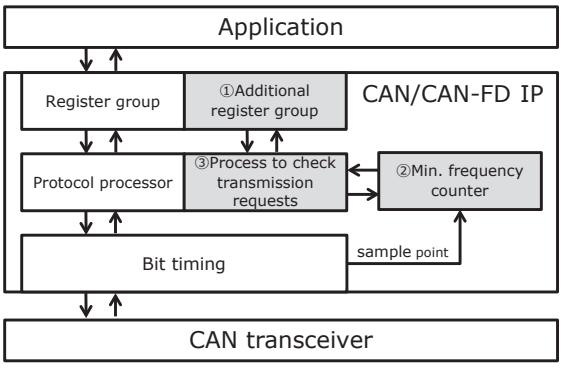


図3　不正送信防止機構の実装

5. 評　　価

5−1　評価方法

本評価では、以下の2つの観点で評価を行った。まず1点目として、追加された不正送信防止機構によるオーバーヘッドについて評価する。不正送信防止機構はハードウェアで実装されているものの、追加された検査処理により、既存するCANコントローラよりも送信要求処理から送信開始までの待機時間が増加する。このため、この増加時間が許容できない時間でないことを確認する。

2点目に、本提案手法による有効性を示すために、不正なプログラムに書き換えられた場合における不正送信防止機構の効果について評価する。プログラムが書き換えられた場合に、不正送信防止機構が有効に働くことを実証する。

5−2　処理オーバーヘッドの評価

本稿で提案する不正送信防止機構を搭載したCANコントローラIPは、既存するCANコントローラIPよりも送信要求時のフィルタリングに要する時間だけ、オーバーヘッドが存在する。このため、ハードウェアカウンタを使用しオーバーヘッドの処理を測定した。送信要求検出後、**図1**の検査処理に関わる時間は最大6.25マイクロ秒であり、CANの転送速度500kbpsにおける3ビット時間から4ビット時間程度の遅延時間に収まることを確認した。この結果から、既存するCANコントローラIPよりもオーバーヘッドが存在するものの、検査処理に関わる時間が周期送信されるCANメッセージの送信周期に比べ、十分に小さいことを確認した。

5−3　不正送信防止機構の評価

(1) 不正に書き換えられたECUによる不正CANメッセージの送信防止

不正送信保護機構が搭載されたCANコントローラを使用する場合、ECU上のプログラムが書き換えられたとしても、ホワイトリストに登録されているCAN-IDのCANメッセージしか送信することができない。この性質を確認するために、アプリケーションから任意のCAN-IDを送信要求するプログラムを作成し、ホワイトリストに登録されたCANメッセージのみが送信されていることを確認した（**図4**、**図5**）。

(2) 不正に書きかえられた踏み台ECUによるCANネットワーク上への送信頻度抑止

提案する不正送信保護機能において、最低送信頻度をホワイトリストに保持することから、不正にプログラムを書き換えられた踏み台となるECUからのDenial of Service attack（DoS攻撃）を抑止することが可能となる。具体的な例として、あるCANメッセージの最低送信周期を5ミリ秒と設定する場合、この5ミリ秒の期間には、1つのCANメッセージしか送信することができない。ただし、このECUの送信メッセージが複数存在する場合には、送信メッセージの数とそれらの最低送信周期の設定値に依存しており、必ずしもDoS攻撃対策として有効であるとは限らないため、最低送信周期の設定方法には注意が必要となる。

ここで、本評価において、およそ10マイクロ秒単位で送信要求するアプリを作成し、ホワイトリストを設定した。CANネットワーク上の不正送信防止機構がない場合には、送信要求の頻度とCANバスでの転送時間間隔に応じて常に送信が繰り返される結果となり、DoS攻撃が可能となる。一方、不正送信防止機構がある場合には、その最低送信周期時間はインターバルが空くため、DoS攻撃に対して効果があることを確認した（**図6**）。

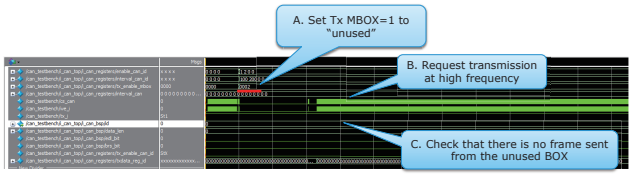


図4　保護機能1の確認

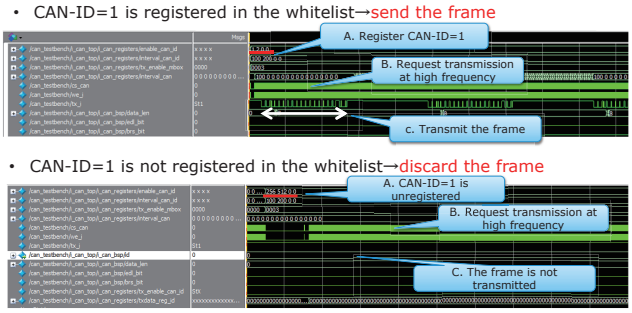


図5　保護機能2の確認

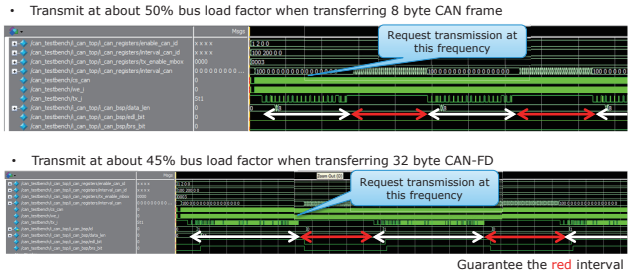


図6　保護機能3の確認

6. 考　　察

6−1　不正送信防止機構の有効範囲

本稿で提案する不正送信防止機構では、正規ECUのプログラムの改ざんを防ぐことはできない。しかしながら、不正にプログラムが書き換えられたECUによる、なりすましメッセージの送信については、ある一定の条件で防ぐこと

が可能である。このため、最善の策としてはセキュアブートと本稿で提案する不正送信防止機構を搭載したCANコントローラを実装することが望ましい。一方で、セキュアブートを実装するには既存するECUにセキュアエレメントを実装する必要があるなど、車載制御システムに存在するすべてのECUで実装するにはコストが高くなり、且つ起動時間におけるオーバーヘッドが懸念される。このため、**表1**に示すように、特に制御に関わる、あるいは外部に接続されるECUには両方の機能を搭載することが望ましい。また、安全性に関わるため、制御系やボディ系の一部のシステムは、セキュアブートあるいは不正送信防止機構のいずれかを選択して適用することが考えられる。

表1　セキュアブートとの組み合わせによる保護

ECU Lv	Secure boot	不正送信防止機構	適用例
Level 1	必要	必要	GW, Engine ECU, H/Uなど
Level 2	不要	必要	制御系、ボディ系の一部のシステムなど
Level 3	不要	不要	一部のサブシステム

6－2　既存研究との比較

これまでに、車載制御ネットワークの侵入検知システム（Intrusion Detection System：IDS）として、Otsuka[7]らがソフトウェアで簡易に実装可能なシステムを提案している。本手法は、車載システムにおいて、各CANメッセージが周期的に送信される性質に着目し、各メッセージの到着間隔をソフトウェア上のアプリケーションで監視する方法である。また、Muter[8]らが、エントロピーベースでのIDSシステムを提案した。しかしながら、車載制御システムを構成するECUでは、低速なコスト効率の高いCPUが搭載されているため、高度な演算処理などを実現することは非常に難しいと考えられる。また、Miller[4]らも、送信頻度を監視する方法について言及している。

関口らが、ホワイトリストを用いたハブの動作について提案しているが、ホワイトリスト・ハブの更新方法などは明確にされてはいない[9]。また、提案手法はハブの構成を対象としており、CAN通信用のポートが1つであるECUについては対象としていない。Ujiieらは、外部からの通信を静的なフィルタを設定することにより、ソフトウェアでフィルタリング（ファイアーウォール機能）を提案している[10]。本手法ではセキュアブートについて言及しているものの、マルウェアに感染される可能性がある車載インフォテイメントシステムに対する有効性については言及されていない。

また、Herberらが、CANバスへのアクセスを時分割にすることにより、DoS攻撃への影響を最小化する方法を提案している[11]、[12]。しかしながら、本手法では、マルウェアの感染によるDoS攻撃の影響を局所化することは可能であるものの、不正なCANメッセージの送信ついては言及されていない。

これらの理由から、複数のアプリケーションを搭載するH/Uやナビゲーションシステムのような場合には、我々の手法が有効と考えられる。

7.　結　　言

本稿では、車載制御システムに用いられるECU上のCANコントローラのハードウェアを拡張することにより、ECUのプログラムが不正なプログラムに改ざんされた場合でも、CANネットワークを保護するためのハードウェアによる不正送信防止機構を提案した。FPGA上に不正送信防止機構を実装し、評価を行った結果、既存する攻撃事例に対して有効であることを確認した。また、踏み台ECUによるCANネットワークへの影響を最小限にする能力があることを示した。

用 語 集

※1　　マルウェア

不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称で、コンピュータウイルスやワームなどがある。

※2　　ホワイトリスト

注意・警戒の必要があるか否かを示す一覧（リスト）のうち、特に注意・警戒が不要である対象を列挙したリストのこと。

※3　　DoS攻撃

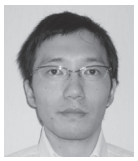
攻撃者が意図的に過剰な通信負荷をかける妨害攻撃のこと。

参 考 文 献

(1) J. Leohold, Communication Requirements for Automotive Systems, 5th IEEE Workshop Factory Communication Systems (2004)
(2) International Organization for Standardization, Road vehicles - Controller area network (CAN) - Part 1: Data link layer and physical signaling, ISO11898-1 (2003)
(3) K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, xperimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy (2010)
(4) C. Valasek, C. Miller, "Adventures in Automotive Networks and Control Unit," http : //www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf (2014)
(5) C. Miller, C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," http://illmatics.com/Remote¥%20Car¥%20Hacking.pdf (2015)
(6) Metromile, https : //www.metromile.com/insurance/ (2015)
(7) Otsuka S., Ishigooka T., Oishi Y., and Sasazawa K., "CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems," SAE Technical Paper 2014-01-0340, 2014, doi:10.4271/2014-01-0340
(8) Muter, M. and Asaj, N., "Entropy-based anomaly detection for in-vehicle networks," In Intelligent Vehicles Symposium (IV), Baden Baden, Germany (2011)
(9) 関口大樹、向達泰希、吉岡克成、松本勉、「不正CANデータ送信を抑制するホワイトリスト・ハブ」、電子情報通信学会SCIS 2014 (2014)
(10) Y. Ujiie, T. Kishikawa, T. Haga, H. Matsushima, T. Wakabayashi, M. Tanabe, Y. Kitamura, J. Anzai, "A Method for Disabling Malicious CAN Messages by Using a Centralized Monitoring and Interceptor ECU," Embedded Security in Cars 2015
(11) Herber, C., Richter, A., Rauchfuss, H., and Herkersdorf, A., "Spatial and Temporal Isolation of Virtual CAN Controllers," In Workshop on Virtualization for Real-Time Embedded Systems (VtRES 2013), pp. 7-13 (2013)
(12) Herber, C., Reinhardt, D., Richter, A., and Herkersdorf, A., "HW/SW Trade-offs in I/O Virtualization for Controller Area Network," presentation at DAC '15 (June 2015)

執 筆 者

上田　浩史*：㈱オートネットワーク技術研究所
グループ長



倉地　　亮*：名古屋大学　特任准教授
博士（情報科学）

本田　晋也：名古屋大学　准教授
博士（工学）

高田　広章：名古屋大学　センター長・教授
博士（理学）

足立　直樹：㈱オートネットワーク技術研究所

宮下　之宏：㈱オートネットワーク技術研究所
室長

*主執筆者