車載ネットワーク侵入検知システム

Intrusion Detection System for In-Vehicle Networks

濱田　芳博*
Yoshihiro Hamada

井上　雅之
Masayuki Inoue

足立　直樹
Naoki Adachi

上田　浩史
Hiroshi Ueda

宮下　之宏
Yukihiro Miyashita

畑　洋一
Yoichi Hata

2015年に報告されたジープチェロキーに対するサイバー攻撃では、遠隔からなりすましメッセージを車載ネットワークに注入することで車両が不正制御された。コネクティッド・自動運転時代に向けて、車載ネットワークでのセキュリティ対策は重要な課題である。車両においてサイバー攻撃に対する具体的な対策を講じるためには、時々刻々と変化する攻撃をいち早く検知する必要がある。本稿では、車載ネットワークに混入されたなりすましメッセージを、セントラルゲートウェイにおいて検知するための侵入検知システムについて提案するとともに、車載ネットワークのトラフィックデータを用いて評価した検知性能について報告する。

In light of the security incident of the Jeep Cherokee in 2015, where a vehicle was illegally controlled remotely using spoofing messages uploaded via a public mobile network, security measures have become one of the most crucial issues in the realization of autonomous driving and connected cars. Taking security measures for each unknown cyber-attack requires quick detection of attacks that will happen throughout the life cycle of the vehicles. This paper introduces an intrusion detection system (IDS) to detect spoofing messages at the central gateway. In addition, we report on the detection performance of the IDS using actual messages sent from an in-vehicle network.

キーワード：侵入検知システム、車載ネットワーク、未知のサイバー攻撃、セントラルゲートウェイ、セキュリティ

1. 緒　　言

近年の車両は車載制御ネットワークにより接続された70～100台のElectronic Control Unit（ECU）と呼ばれる組み込みコントローラにより制御されるとともに、車両外の様々なサービスとネットワークを介して制御データを共有することで車両の安全性や利便性を向上させている。一方でこのような外部との通信を悪用して、車両を遠隔から不正に制御するサイバー攻撃の可能性が示されており、この対策が急がれている[(1)]。サイバー攻撃に対する適切なセキュリティ対策を行うためには、車両が攻撃を受けたことを検知する必要がある。このための手段として、侵入検知システム（Intrusion Detection System: IDS）が知られている。車両の製品寿命はモデルで考えると10年以上であり、製品設計後に未知のサイバー攻撃を受ける可能性が高いため、車載侵入検知システムではこのような攻撃を検知することが重要である。未知のサイバー攻撃を検知するためには、監視対象の通常状態からの逸脱度合いにより攻撃の検知を行う、アノマリ型の侵入検知システムが有効である。しかし、従来の車載におけるアノマリ型侵入検知方式の研究では、サイバー攻撃により車載ネットワークに挿入されたなりすましメッセージの特定が困難である。挿入されたなりすましメッセージを特定することで、攻撃への対策を実施するまでの時間短縮や、攻撃への対策範囲を限定することが可能である。そこで本稿では、ペイロードに含まれる制御データを監視する検知性能の高いアノマリ型の検知方式を提案し、車載ネットワークにおいて一般的に用いられる、Controller Area Network（CAN）プロトコルでのトラフィックデータを用いて評価した検知性能について報告する。

2. CANプロトコルとセキュリティ脅威

2－1　CANの特徴

CANプロトコルとCAN with Flexible Data rate（CAN FD）プロトコルの2つがある。CANプロトコルはISO11898-1（2003）[(2)]で標準化され、CAN FDプロトコルは同標準を改訂する形でISO11898-1（2015）[(3)]にて標準化された。本プロトコルでは、バス型のトポロジ上の複数のノード（ECU）の内、通信調停により送信権を得たノードが最大8バイト（CAN）または64バイト（CAN FD）のペイロードをブロードキャスト送信することで制御システム用途での低遅延なメッセージの通信を実現している。

2－2　通信特性

CANでのメッセージは、車載ネットワークで一意の識別子であるCAN-IDが付与されたCANフレームにより、2種類のパターンで伝送される。一つは周期的にCANフレームが送信される場合の伝送パターンであり、速度、エンジン回転数やアクセル開度といった主要な制御情報の通知に用いられる。もう一つは非周期的に送信される場合の伝送パターンであり、ドアの開錠・施錠といったイベントの通知

に用いられる。

2−3　ネットワーク構成

CANプロトコルはバス型のトポロジであり、バス一つ当たりのECUの接続台数には上限がある。このため、多くのECUが用いられるシステムでは、**図1 (a)** に示すようにバス間をゲートウェイで中継することにより、ネットワークを構成する。しかしこの場合、複数のゲートウェイがバス間に介在するため、通信遅延が増大する。**図1 (b)** に示すセントラルゲートウェイを用いたネットワークでは、ネットワークを機能系統毎にサブネットワークに分け、これらを単一のゲートウェイにより接続するため、通信遅延が短縮される。

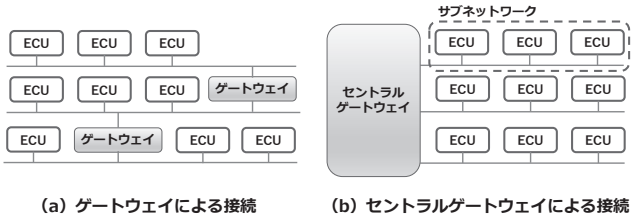


図1　ネットワーク構成

2−4　セキュリティ脅威

KoscherらはCANプロトコルについて次に示す3つの脆弱性を指摘している[(4)]。(1) ネットワーク上の制御情報を容易に解析可能、(2) なりすましメッセージを容易に挿入可能、(3) Denial of Service（DoS）攻撃に弱い。ここで、なりすましメッセージの挿入やDoS攻撃は、**図2**に示すように、CANバスに接続される攻撃ECUを介して行われる。これは、正常なECUのファームウェアを改ざんしたものか、不正なECUを接続したものである。

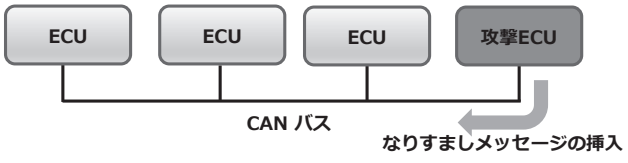


図2　攻撃ECUによるなりすましメッセージの挿入

3.　車載ネットワークのセキュリティ対策

3−1　従来技術

車載ネットワークでのセキュリティ対策に関する研究は以下の2つに分類できる。製品寿命の長い車両では、未知のサイバー攻撃によりセキュア通信が無効化された場合でも、継続的にセキュリティ対策を行うために、侵入検知システムが必要になる。

(A) セキュア通信
　ネットワークプロトコルでのセキュリティ対策。

(B) 侵入検知システム
　ネットワークプロトコルの上位で動作し、アプリケーションやネットワークでの疑わしい動きを検知する。

3−2　侵入検知システム

侵入検知方式には、シグネチャー型とアノマリ型の2種類がある。これらは、監視対象の疑わしい振る舞いを検知することで侵入を検知する。シグネチャー型は、監視対象の誤った使用例を定義し、この定義と一致するものを疑わしい動きとして検知する。アノマリ型は、監視対象の通常時の動作を定義し、この定義から逸脱するものを疑わしい動きとして検知する。未知のサイバー攻撃の検知は、アノマリ型の検知方式においてのみ可能である。

4.　車載侵入検知システム

4−1　開発システム

当社で開発を進めるアノマリ型の車載侵入検知システムは、**図3**に示すように車載ネットワークを構成する要素で分けた3段階の監視レベルを持つ。監視レベルが高くなると監視対象は細分化されるため、攻撃された対象を特定しやすくなり、その結果、攻撃への対策を具体化しやすくなる。しかし、その一方で、システム全体での監視対象の数が増加する。このため、監視レベルが高い監視方式のみでは、メモリ容量やCPU速度などが制限される車載環境において、車載ネットワーク全体の監視が困難になる。当社システムでは、これら3つの監視レベルを組み合わせ、監視レベルの低い方式により、車載ネットワーク全体の監視を行い、監視レベルの高い方式により、車両において重要な特定の対象について監視を行う。

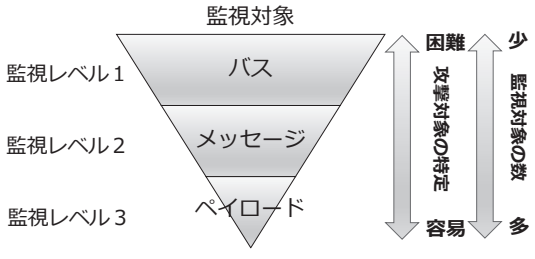


図3　アノマリ型車載侵入検知システム

4−2　従来の車載侵入検知方式の問題点

車載侵入検知の従来方式では、なりすましメッセージの検

知性能の低さが問題である。メッセージの通信特性を監視する従来方式[5]では、サイバー攻撃を受けた場合に、正常メッセージと区別してなりすましメッセージを検知することが難しい。ペイロードに含まれる値が滑らかに変化するセンサ型の制御データを監視する従来方式[6]では、監視対象制御データの僅かな改ざんが繰り返し行われる場合に、なりすましメッセージの検知が困難である。

5. 提案方式

5−1 CDEC

従来の車載侵入検知方式でのなりすましメッセージの検知性能の低さを解決するために、メッセージのペイロードに含まれるセンサ型の制御データを監視するControl Data Estimation for anomaly detection with Correlation data（CDEC）を提案する[7]。CDECでの制御データの監視は、5−2節「アプリケーションモデル」に示すように、監視対象となる制御データに対して相関関係のある、相関制御データ群により行うため、車両内から多くの相関制御データを取得できると、なりすましメッセージの検知性能が向上する。このため、本提案方式は、セントラルゲートウェイのように車載ネットワークの多くのサブネットワークにアクセス可能な位置での監視が望ましい。

5−2 アプリケーションモデル

本提案方式は、**図4**に示すように3つの機能により構成される。分割器では、監視対象制御データと相関関係のある制御データを含むメッセージが受信された際に、ペイロード中の相関制御データを記憶する。推定器では、監視対象制御データを含むメッセージが受信された際に、5−3節「車両データモデル」に示すモデルを介して、記憶している相関制御データ群から、監視対象制御データの推定値を計算する。評価器では、監視対象制御データの推定値の計算を終了した際に、監視対象制御データの現在値と、推定値の差異を、スレッショルドと比較する。差異がスレッショルドの範囲以内となる場合は、監視対象制御データを正常と判定し、超える場合は異常と判定する。

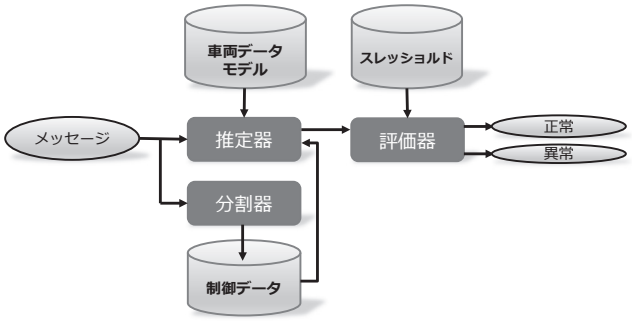


図4 CDECアプリケーションモデル

5−3 車両データモデル

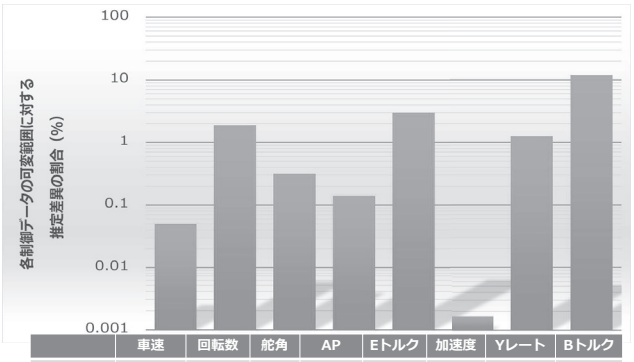
車両データモデルは、監視対象制御データの推定値を相関制御データ群から算出するために用いられる。モデルの学習は2段階で行う。1段階目は相関分析※1であり、車載ネットワークのトラフィックデータから、監視対象制御データに対する相関制御データ群の抽出を行う。2段階目は車両データモデルの学習であり、監視対象制御データと相関制御データ群を用いて、車両データモデルのパラメータを決定する。本提案方式では車両データモデルには、回帰モデル※2を用いる。回帰モデルについては、参考文献 (8)、参考文献 (9) が詳しい。

6. 評　価

6−1 車両データモデルの学習と推定精度

本提案方式に必要な車両データモデルの学習可否と、推定精度について、車両の走行特性を示す8種類のセンサ型の制御データを用いて評価した。各制御データに対する車両データモデルの学習は、5−3節「車両データモデル」に従い、車載ネットワークのトラフィックデータを用いて行った。推定精度の評価指標には、各制御データの可変範囲に対する推定差異の二乗和平均誤差（RMS: Root Mean Square）の割合を用いた。

図5に評価結果を示す。まず、評価対象とした車両の走行特性を示す8種類のセンサ型制御データ全てについて、車載ネットワークのトラフィックデータから、車両データモデルを学習可能であることを確認した。各々の推定精度については、Bトルクでは11.9%、それ以外の7種類では3%未満となることを確認した。



	車速	回転数	舵角	AP	Eトルク	加速度	Yレート	Bトルク
可変範囲	0-180	0-4000	±612	0-100	0-140	±3	±30	±210
推定差異のRMS	0.18	74.9	3.87	0.14	4.16	1e-4	0.76	50.0

※可変範囲は、トラフィックデータからの推定値。

図5 推定精度

6－2　検知性能

なりすましメッセージの検知性能について、2種類の従来方式とともに評価を行った。一つはメッセージの受信間隔を監視する方式であり、もう一つは監視対象制御データの時系列での変動を監視する方式である。後者の従来方式では、過去に受信した正常データを用いて監視対象制御データの現在値を推定し、現在値と推定値の差異が許容範囲を超える場合に、受信したメッセージをなりすましメッセージと判定する。

評価指標には、**式 (1)** に示す感度と、**式 (2)** に示す真陰性率[※3]を用いた。感度が1の場合は、挿入されたなりすましメッセージを全て検知したことを示す。真陰性率が1の場合は、全ての正常メッセージを正しく認識し、なりすましメッセージとして誤検知していないことを示す。各式で用いられる真陽性と偽陽性は、それぞれ、なりすましメッセージを正しく判定した数と、誤判定した数である。真陰性と偽陰性は、それぞれ、正常メッセージを正しく判定した数と、誤判定した数である。

$$感度＝\frac{真陽性}{真陽性＋偽陰性} \quad \cdots\cdots (1)$$

$$真陰性率＝\frac{真陰性}{真陰性＋偽陽性} \quad \cdots\cdots (2)$$

本評価では、**図6**に示す攻撃モデルを用いて、車速データ（約60km/h）が繰り返し送信される中、速度を81km/hに改ざんするために、2種類の攻撃方法により攻撃ECUから、なりすましメッセージを繰り返し送信した。一つ目の攻撃方法は、ストレート攻撃である。**図7上段**に示すように、改ざんする速度の81km/hを繰り返し送信する。二つ目の攻撃方法は、ジャブ攻撃である。**図7下段**に示すように、正常データの60km/hから改ざん目標速度の81km/hまで、1.5km/hずつ僅かに速度を増加させた改ざんデータを14回に分けて送信した後、81km/hの改ざんデータを繰り返し送信する。**図8**に、ジャブ攻撃での速度データの全体像を、可視化のためにサンプルを間引いて示す。**図8 (A)** は、ジャブ攻撃が行われた区間であり、**図7下段**はこの区間の先頭部分を拡大したものである。ストレート攻撃での速度データの全体像は、攻撃開始時の改ざんデータを除いて、ジャブ攻撃と同様である。

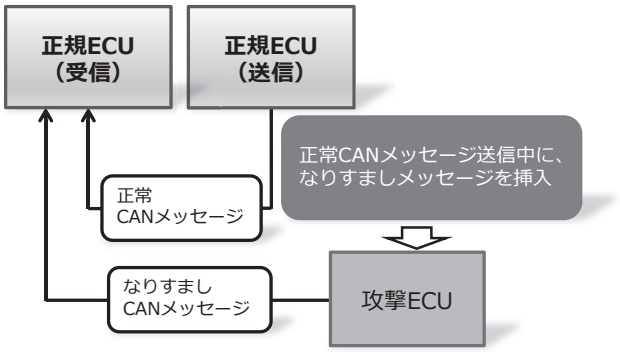


図6　攻撃モデル

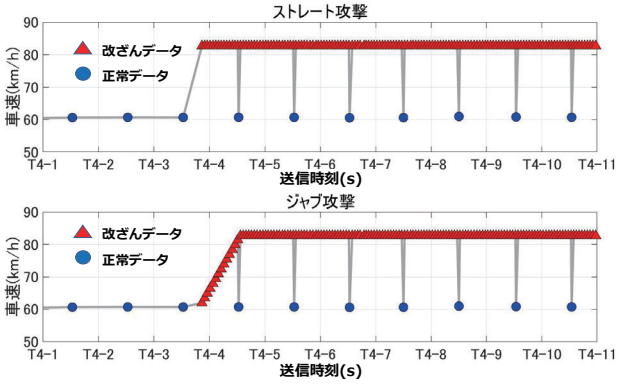


図7　攻撃種類

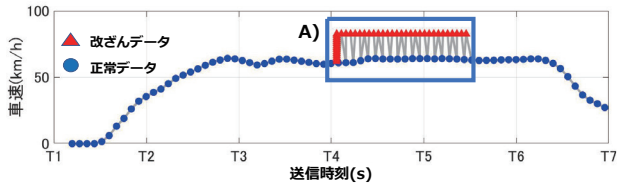


図8　ジャブ攻撃を加えた速度データの全体像

図9に評価結果を示す。メッセージの受信周期を監視する従来方式では、ストレート攻撃、ジャブ攻撃、何れも感度は1となった。しかし、真陰性率は0.7と大きく低下した。この従来方式は、メッセージの受信間隔の許容範囲内に正常メッセージとなりすましメッセージを受信する場合には、メッセージの区別がつかなくなるため、正常メッセージも含めてなりすましメッセージと判定するためである。本評価では、正常メッセージとなりすましメッセージが混じりあって受信される**図8 (A)** において、この従来方式での真陰性率の低下を確認した。

監視対象制御データの時系列での変動を監視する、従来方式でのストレート攻撃に対する検知性能は、感度、真陰性率ともに1であった。しかし、ジャブ攻撃において感度が0、真陰性率が0.5と検知性能が大きく低下した。これは、ジャブ攻撃が開始され、速度が正常データの約60km/hから改ざん目標速度の81km/hまで、1.5km/hずつ僅かに速度を増加させながら繰り返し改ざんされる場合、過去に正常と判定した速度データを用いて現在の速度を推定すると、改ざんデータとの差異は許容範囲内となるため、受

信したなりすましメッセージ全てが正常メッセージと誤判定されたこと。さらに、速度が81km/hまで改ざんされた後は、過去に正常と判定した改ざんデータから現在の速度を推定すると、正常データの約60km/hとの差異は許容範囲を超えるため、全ての正常メッセージがなりすましメッセージと誤判定されたことが原因である。

提案方式では、両攻撃に対して、従来方式よりも高い検知性能を示した。ストレート攻撃に対する検知性能は、感度、真陰性率ともに1であり、ジャブ攻撃では感度、真陰性率ともに0.99であった。ジャブ攻撃で僅かに発生した誤判定は、攻撃開始直後の1度である。これは、なりすましメッセージにより挿入された改ざんデータの値が、車両データモデルでの推定差異以下となったために発生した。しかし、なりすましメッセージにより挿入される改ざんデータの値は、81km/hに到達するまで1.5km/hずつ徐々に大きくなる。本評価では、2つ目以降のなりすましメッセージが持つ改ざんデータは、車両データモデルの推定差異を超えたため、全てをなりすましメッセージとして検知した。本提案方式では、車両データモデルを介して相関制御データ群により間接的に監視対象制御データの監視を行うため、ストレート攻撃に加えて、ジャブ攻撃も検知可能であることが本評価により示された。

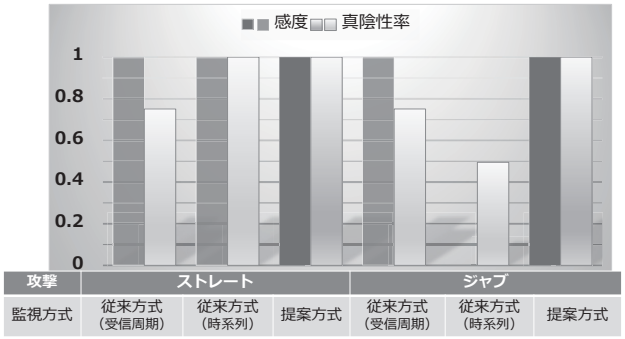


図9　検知性能

7. 結　　言

車載ネットワーク用のアノマリ型侵入検知方式CDECについて提案を行った。本提案方式では、センサ型の制御データの監視を、相関関係にある制御データ群から車両データモデルを介して推定した値と比較することで行う。

評価では、車両の走行特性を示す8種類のセンサ型の制御データに提案方式を適用し、全てにおいて車両データモデルをトラフィックデータから学習可能であることを確認した。また、車両データモデルの推定精度は、7種類のデータについて3%未満となることを確認した。さらに、提案方式と2種類の従来方式のなりすましメッセージの検知性能を比較した。この結果、提案方式の検知性能が最も高く、なりすましメッセージを挿入された場合でも、正常メッセージと区別して検知可能であることを確認した。

本提案方式によれば、サイバー攻撃により車載ネットワークに挿入されたなりすましメッセージの特定が可能である。そのため、攻撃対象を特定しやすく、これにより、攻撃の対策を行うまでの時間短縮や、対策範囲の限定を行える。当社で開発を進める侵入検知システムは、車載ネットワークに対する3段階の監視レベルを、本提案方式や比較に用いた従来方式等を用いて構成することで、製品寿命の長い車両への未知のサイバー攻撃の検知を、車載環境で実現する。

用 語 集

※1　　相関分析

2つの変数間（x,y）の相関関係を**式 (3)** に示すピアソンの積率相関係数の式により求める。rは相互相関係数であり、xとyは各々監視対象制御データとその他の制御データの値である。μ_xとμ_yは各々監視対象制御データと他のその他のデータの平均値であり、nはサンプル数である。相互相関係数は0～±1.0の範囲で変化し、値が1.0または-1.0に近い程2つの変数間の相関関係が強く、0.4以上、-0.4以下で相互に相関関係がある。

$$r = \frac{\sum_{i=1}^{n}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{n}(x_i - \mu_x)^2}\sqrt{\sum_{i=1}^{n}(y_i - \mu_y)^2}} \quad \cdots\cdots\cdots\cdots (3)$$

※2　　回帰モデル

統計的な方式により算出される目的変数と説明変数間の関係式。本稿では目的変数は監視対象制御データであり、説明変数は監視対象制御データに対して相関関係のあるその他の制御データである。

※3　　真陰性率

検知性能に対する評価指標の一つ。正常メッセージを正しく識別した割合を示す。1が理想的な値である。

参 考 文 献

(1) Miller, C., and Valasek, C., "Remote Exploitation of an Unaltered Passenger Vehicle," presented at DEF CON 23 (August 2015)
(2) International Organization for Standardization, "Road vehicles-Controller area network (CAN) - Part 1 : Data link layer and physical signaling," ISO11898-1, Rev. (2003)
(3) International Organization for Standardization, "Road vehicles-Controller area network (CAN) - Part 1 : Data link layer and physical signaling," ISO11898-1, Rev. (2015)
(4) Koscher, K., Czeskis, A., Roesner, F., Patel, S. et al., "Experimental Security Analysis of a Modern Automobile," *2010 IEEE Symposium on* Security and Privacy (2010)
(5) Hamada, Y., Inoue,M, Ueda, H., Miyashita, Y, et. al., "Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks," SAE International Journal of Transportation Cybersecurity and Privacy, Vol1 (2018)
(6) Müter, M., and Asaj, N., "Entropy-Based Anomaly Detection for In-Vehicle Networks," *2011 IEEE Intelligent Vehicle Symposium (IV)* (2011)
(7) Hamada, Y., Inoue, M., Tateishi, H., Adachi, N., et. al., "Virtual Secsing Anomaly Detection for In-Vehicle Network," 2018 Symposium on Cryptography and Information Security (January, 2018)
(8) Tibshirani, R., "Regression shrinkage and selection via the lasso," Journal of the Royal Statistical Society. Series B (Methodological), pp. 267–288 (1996)
(9) Breiman, L., Friedman, J., Stone, C.J., and Olshen, R.A., "Classification and Regression Trees," Boca Raton : Chapman and Hall/CRC, Monterey, CA (1984)

執 筆 者

濱田　芳博*：サイバーセキュリティ研究開発室 主査

井上　雅之：㈱オートネットワーク技術研究所 主席

足立　直樹：㈱オートネットワーク技術研究所

上田　浩史：㈱オートネットワーク技術研究所 グループ長

宮下　之宏：㈱オートネットワーク技術研究所 室長

畑　　洋一：サイバーセキュリティ研究開発室 室長

*主執筆者