URL　https://journal.ntt.co.jp/article/30150
DOI　https://doi.org/10.60249/24115103

車両SOCに関するNTTセキュリティ・ジャパンの取り組み

コネクティッド技術の進化やさまざまなモビリティサービスの誕生・拡大を背景に，車両がサイバー攻撃の脅威にさらされるリスクが高まっており，それを受けてレギュレーションの制定もされています．これらに対応するため，車両を監視しサイバー攻撃を検知する車両SOC（Security Operation Center）のニーズが高まっています．本稿では，NTTセキュリティ・ジャパンによる車両SOCに関する取り組みについて紹介します．

キーワード：#車両SOC，#コネクティッドカー，#セキュリティ

これとう　ひろき
是洞　博紀

NTTセキュリティ・ジャパン

車両SOCとは

SOC（Security Operation Center）とは，監視対象に対するサイバー攻撃を検知し，通知し，サイバー攻撃への対応を支援する組織のことです．SOCの主な監視対象は企業のIT環境ですが，通常のIT環境とは異なる車両を監視対象とするものを車両SOC，もしくはVSOC（Vehicle SOC）と呼びます．車両SOCは，車両に搭載されたセキュリティセンサのログ，OEM（Original Equipment Manufacture：自動車製造者）の車両向けサービス基盤における各種ログ，および車両ネットワークトポロジーなどの監視対象の車両の情報を用いて分析を行い，車両に対するサイバー攻撃を検知し，通知します．車両SOCの想定顧客としては，OEMのほか，車載電子制御機器や部品の製造者などのサプライヤ，カーシェアなどのMaaS（Mobility as a Service）プロバイダ，タクシーなどのFleet事業者，自家用車のユーザ，保険会社などが挙げられます．

車両SOCが求められる背景

車両SOCが求められる背景には，車両がサイバー攻撃の脅威にさらされるリスクの高まりと，それらを背景とするレギュレーションの制定があります．

コネクティッド技術の進化や多様化するお客さまニーズを背景に，自動車のデータを活用したモビリティサービスが次々と誕生・拡大しています．これらのサービスには，OEMが提供するもの，OEM以外のサードパーティが提供するものがあり，さまざまなIoT（Internet of Things）機器と同様に車両もインターネットにつながるようになってきました．利便性が増す反面，サイバー攻撃の脅威にさらされるリスクも高まっています．

車両に対するサイバー攻撃の脅威の例としては，トヨタ自動車のプリウスなどを例に専門家がハッキング手法を披露（2013年），専門家がJeepのハッキング可能な脆弱性を発表（2015年），テスラModel Sのキーレスエントリーシステムをハッキングし盗み出す様子をとらえた監視カメラ映像の公開（2018年），などがあります．このうち，2015年のJeepの事例では，サイバーセキュリティの専門家がFCA社の無線通信サービス「Uconnect」を介してJeep CherokeeのECU（Electronic Control Unit：車両のシステムを制御する装置）を攻撃することで，エンジンやステアリング，ワイパーを自在に操れる脆弱性を発表したことを受け，FCA社がリコールを実施しました．すでに市場にある車両に対して攻撃可能なことを示す事例になります．企業の株価に大きな影響が生じる事態となり，業界全体が本格的にセキュリティ対策に乗り出す契機になりました．

こうしたリスクの高まりを背景に，世界規模でレギュレーションが制定されています．国連が発行したサイバーセキュリティマネジメントシステムに関するUNR-155，ソフトウェア更新に関するUNR-156に基づき，日本を含む加盟各国にてサイバーセキュリティ対策が義務化されてきています．**図1**に示すとおり，UNR-155ではCSMS（Control Systems Security Management Systems）の導入や，車両型式要件として車両に対するサイバー攻撃の監視等が求められています．

ここで述べた車両に対するサイバー攻撃の脅威の高まりと法規対応が，自動車製造者やサプライヤが車両SOCを導入する主な動機となっています．

車両SOCのサービス企画

車両SOCのニーズにこたえるために，NTTセキュリティ・ジャパンはNTTコミュニケーションズの車両向けセキュリティ監視サービスの提供に向けた取り組みに貢献しています．

このサービスでは，①車両に搭載されたセキュリティ機器から出力されるログやコネクティッドサーバとの通信ログによる車両の監視とサイバー攻撃の検知，およびサイバー攻撃の動向や実際に車両へ行われた攻撃内容を把握することによる高度化・巧妙化する攻撃への対応，②サイバー脅威の分析結果および復旧対応に資する情報のお客さまへの提供，③グローバル規模での安定した車両セキュリティ監視，をめざしています．

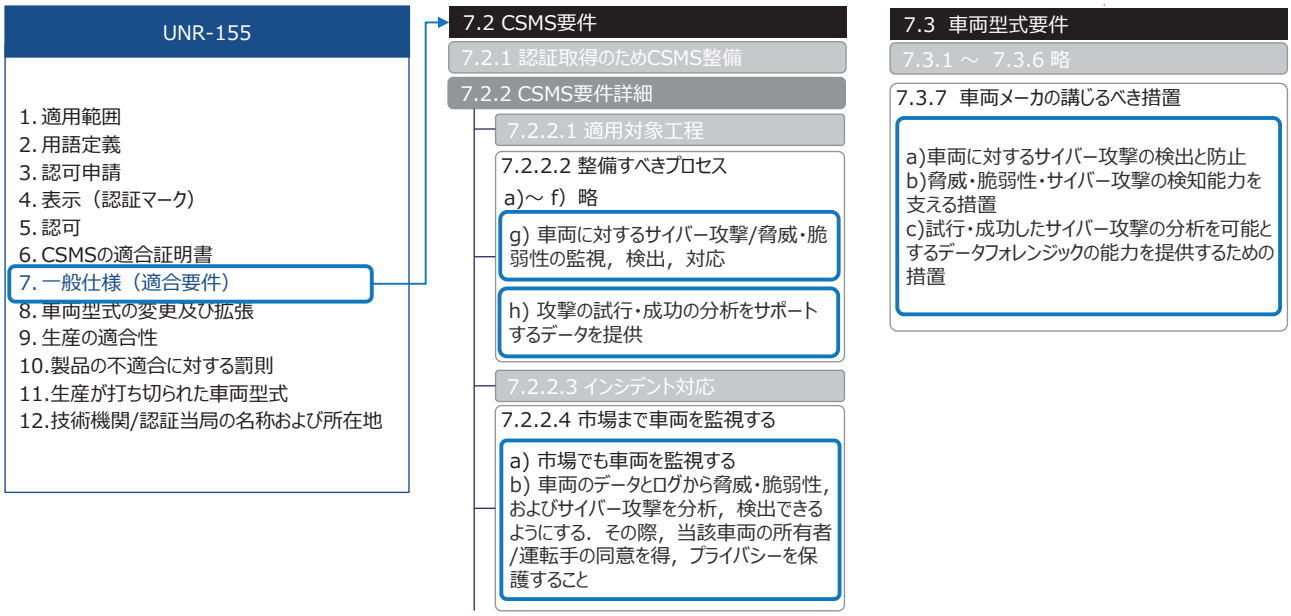


図1　UNR-155 サイバー攻撃の監視等に関する要件概要

車両SOCサービスに対する貢献

車両SOCとIT向けSOC（ITSOC）には類似点があります．NTTセキュリティ・ジャパンが長年培ってきたITSOC提供事業者としての知見とノウハウが，車両向け監視サービスの開発と提供に大きく貢献すると考えています．

攻撃検知の知見と高度な技術（分析基盤），人材（分析官）は代表的なものですが，サービスの継続的な提供にはさまざまな役割の要員が必要です．そして，それぞれの役割の要員がサービス提供を継続するための業務プロセスがあります．例示すると，顧客から受領するログを分析し攻撃検知結果を通知する業務，顧客に提供したレポートに対する問合せに対応する業務，サービス提供の分析基盤の稼働状況を監視し安定運用をする業務，SOCが発見した脅威やインシデントへの対応業務，分析基盤の高度化や改善を行う業務，分析基盤の保守・運用業務，顧客への各種通知・問合せ受付業務，などです．これらは車両SOCとITSOCに共通で必要です．

NTTセキュリティ・ジャパンはITSOCのサービスを20年以上提供してきた実績に裏付けされたSOC業務に関する知見とノウハウがあり，サービス開発における業務，プロセス，および体制策定の中心的役割を担っています．

これらに対応する人材の観点では，ITSOCの開発と提供の知見，技術を持つ人材が数多く在籍しています．車両への攻撃の検知に活用できる脅威情報，攻撃検知手法，攻撃手口や攻撃者の行動，ソフトウェアやネットワークの技術，計算機科学・通信技術，マルウェア解析能力，高度な脅威検知システムの開発・構築能力，企業やOT（Operational Technology）向けセキュリティセンサへの深い知見を持った人材がおり，サービス開発や提供において分析基盤開発や分析業務を担っています．

次に，車両SOCがITSOCに対し特異な点と取り組み例について紹介します．

1点目は，車両SOCの顧客がOEMのPSIRT（Product Security Incident Response Team）である場合，同組織は製品の品質責任を担うためインシデント対応を支援する情報提供を要望される点です．要望の例としては，サイバー攻撃の被害を受けた車載機器の特定や被害を受けた車両以外の車両への影響評価等が挙げられます．この点に対しては，OEMから受領するデータを用い，被害を受けた車載機器を特定する仕組みの具体化に貢献しています．

2点目は，IT環境と異なり，監視対象システムの構成が標準化・類型化されていない（OEM，車両モデルごとにシステム構成が大幅に異なる）という点です．これにより，(1) 攻撃成功の要因と影響範囲特定の難易度が大きく上がる，(2) 分析ロジックは監視対象の種別ごとに開発・更新・運用する必要がある，という点です．

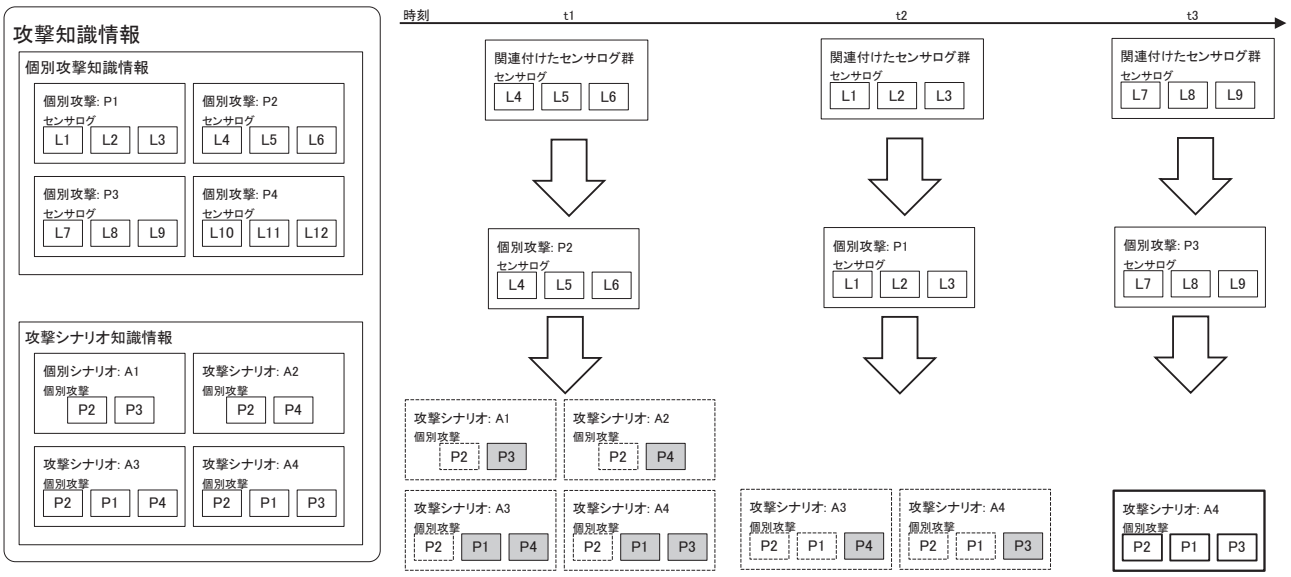


図 2　個別攻撃 攻撃シナリオ分析処理例

（1）の課題に対し，攻撃成功の要因と影響範囲の特定を容易にするために，複数の段階・手段から構成される攻撃を一連のもの（攻撃シナリオ）としてとらえる技術の開発を実践しました．具体的には，①攻撃を構成する段階・手段の具体的な知識に基づき，攻撃を構成する段階・手段を検知するロジック（個別攻撃検知ロジック）を備えておく，②当該攻撃を構成する段階・手段の知識に基づく攻撃検知ロジック（攻撃シナリオ検知ロジック）を備えておく，③センサログと個別攻撃検知ロジックに基づき，攻撃を構成する段階・手段（個別攻撃）の発生を検知すること，④検知した複数の攻撃と攻撃シナリオ検知ロジックに基づき，複数の攻撃から構成される攻撃（攻撃シナリオ）の発生を検知する，というものです（**図 2**）．

（2）の課題をさらに分解すると，（2）- 1 監視対象の種別（差異）を具体的，詳細な理解，（2）- 2 実行すべき分析ロジックが大量となり，分析性能（処理時間・スループット）への懸念，となります．

（2）- 1 の課題に関しては，監視対象の車両の仕様の理解を進め，開発を進めています．

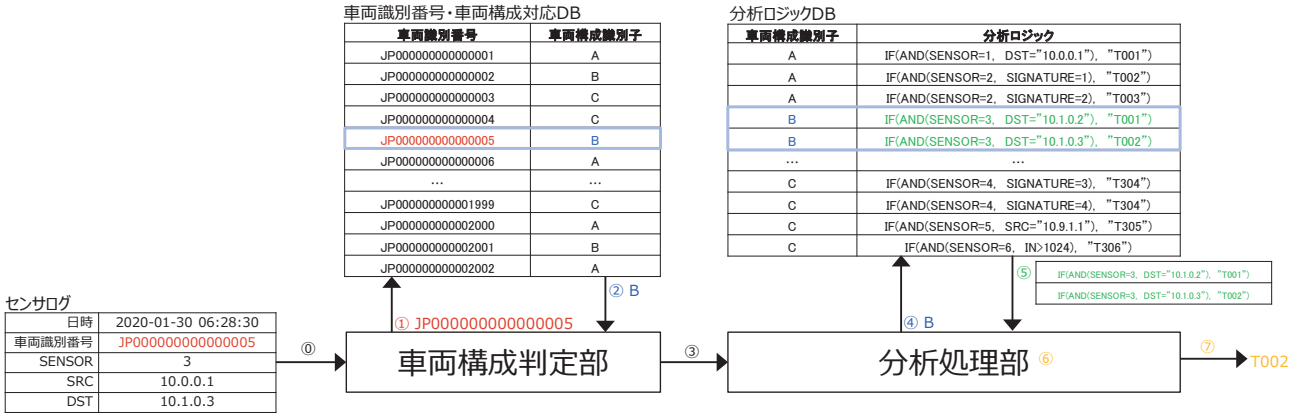
（2）- 2 の課題に対し，車両のセンサログから車両構成を検索・特定し，特定した車両構成に対応する分析ロジック群を実行して分析結果を得る技術の開発に貢献しました．センサログごとに実行する分析ロジックを限定することにより，実行する分析ロジックを限定しない場合に比べ，分析負荷が効率化され，分析性能（処理時間・スループット）の向上が期待できます（**図 3**）．

3 点目は，車両からのデータの通信可用性が速度の観点で断続的・低速であること，データ送信には遅延のリスクがある点です．この点については，データが遅延・欠損しても分析を実行できる仕組みの開発を行っています．

その他，車両SOCにおいて攻撃検知等のために実行する分析処理を効率化し，CPUやメモリなどの計算資源の消費を抑制するための技術や，サイバー攻撃に起因しない事象に基づき発生したセンサログを排除することにより，無駄な分析処理の抑制と攻撃検知の精度向上効果を期待できる技術を開発しました．

今後の課題と展望

前述のとおり，車両SOCのニーズは高まっていますが，現時点で顕在化しているサイバー脅威による車両の被害事例は，ITと比べると少なくみえます．これは現時点の話であって，楽観視してよいものではありません．市場のコネクティッドカー（ICT端末としての機能を有しインターネットへの接続機能を有する車両）がますます増加し，機能のIT化が進展することにより，IT環境と同様に脅威が格段に増えることが想像されます．そのような状況での課題は，今後想定される新たな脅威へ対応するための組織・人的能力を有し備えることです．NTTセキュリティ・ジャパンには計算機



⓪ 車両構成判定部が分析対象となるセンサログを受領する
① 車両構成判定部は，車両識別番号(JP000000000000005)を検索キーとして，車両識別番号・車両構成対応DBを検索する
② 車両構成判定部は，車両識別番号(JP000000000000005)に対応する車両構成識別子(B)を得る
③ 車両構成判定部は，センサログ，および当該センサログに対応する車両構成識別子(B)を分析処理部に渡す
④ 分析処理部は，車両構成識別子(B)を検索キーとして，分析ロジックDBを検索する
⑤ 分析処理部は，車両構成識別子(B)に対応する分析ロジック群を得る
⑥ 分析処理部は，車両構成識別子(B)に対応する分析ロジック群を上記センサログを入力として実行する
⑦ 分析処理部は，分析ロジック群の実行結果(T002)を出力する

図３　車両構成に対応する分析ロジック群を実行して分析結果を得る処理

科学や通信工学を基礎とする人材が多数在籍しており，それらの技術的基礎を活用し，エンタープライズITシステムとは異なる脅威が想定されるOTのお客さま向けにもサービスを開発し提供している実績があります．

NTTセキュリティ・ジャパンは，これまで培ってきたITSOCでの日々の検知と分析結果，20年以上グローバル規模で収集・開発し磨き上げ続けているインテリジェンスを活用した脅威への迅速な対応，および自社にソフトウェア開発者・組織を保有することで，分析能力，分析基盤（ロジック含む）の環境変化や新たな脅威に対し柔軟・迅速な対応をすることに貢献していきます．

是洞　博紀

本稿で紹介した事項や，NTTセキュリティ・ジャパンにおけるその他の車両SOCの取り組みに関して興味がある方は，お問い合わせください．

◆問い合わせ先

NTTセキュリティ・ジャパン
営業本部マーケティング部
E-mail　nsj-pr @ security.ntt