別紙

# 「IoTセキュリティ基盤を活用した安心安全な社会の実現に向けた実証実験」の結果の公表

総　　務　　省
情　報　流　通　行　政　局
サイバーセキュリティ課

平成30年６月

# 実証実験の背景と検討事項



○　近年、IoT機器が急速に普及し、各種サービスへの展開が期待される一方、IoT機器に対するサイバー攻撃も年々増加・巧妙化しており、**IoT機器やIoTサービス特有の性質を踏まえたセキュリティ対策は急務**。

○　IoT 機器単体では必要なセキュリティ対策の実現が困難な場合や、IoT 機器に精通していない利用者についてはセキュリティ対策が十分に講じられない場合が想定されることから、**ネットワーク側で一元的にセキュリティ対策を講ずる仕組みの確立も必要**。

○　**IoT機器とインターネットの境界上にIoTセキュアゲートウェイを設置し、その有用性に関する実証実験を実施。**

【検討事項】

①　IoT機器をネットワークに接続する際の認証や暗号化とIoT機器の管理

②　IoT機器から収集したデータの分析

③　問題が生じた場合の原因特定と対処

**（参考）「IoTセキュリティ総合対策」（平成29年10月サイバーセキュリティタスクフォース）（抜粋）**

Ⅱ 具体的施策

（1）脆弱性対策に係る体制の整備

③ IoTセキュアゲートウェイ

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、流通している機器の中から、脆弱性を有する機器を完全に排除することは困難であることから、機器の設置(ネットワークへの接続)段階において、脆弱性を有する機器が存在することを前提として、セキュアなシステム構築を実現する仕組みが重要となる。また、IoT機器単体では必要なセキュリティ対策の実現が困難な場合やIoT機器に精通していない利用者についてはセキュリティ対策が十分講じられない場合が想定される。このため、IoTシステム・サービス全体としてセキュリティを確保する観点から、IoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組について、総務省において実証を進めるとともに、セキュリティ評価や実際の導入を進める仕組みについて検討する必要がある。

# IoTセキュアゲートウェイ実証実験の概要

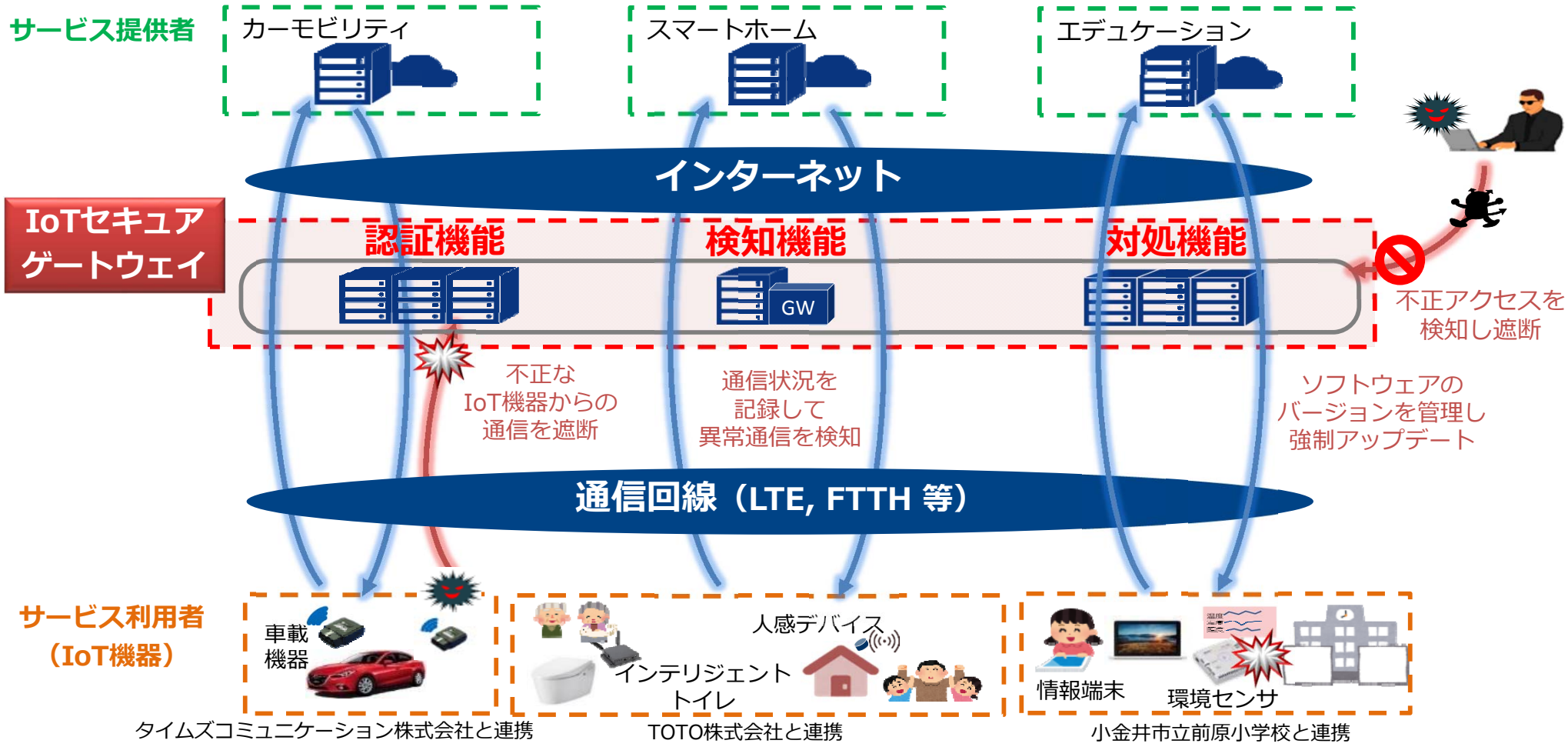


○　実証実験では、様々なセキュリティ脅威に対して、**認証、検知、対処といった一連のセキュリティ対策**ができるかを試行。

- **認証**（IoTサービスに接続しようとするIoT機器が正当なものであるかをIoTセキュアゲートウェイにおいて認証）
- **検知**（データ受信頻度や通信量等を基に、異常な通信を検知）
- **対処**（異常な通信を行うIoT機器の遮断や、脆弱性を有するIoT機器の自動ソフトウェアアップデート）

## 実証実験のイメージ

実施主体：NTTコミュニケーションズ株式会社



# 実証実験を実施した分野



○　IoT機器を通じて得られるデータ・情報を用いたサービスの展開が進む、カーモビリティ分野、スマートホーム分野、エデュケーション分野の三つを選定し、実証実験を実施。

○　IoT機器を利用したサービスを提供する際のリスクとして、不正アクセス、なりすまし、乗っ取り、盗聴、盗難を想定し、各分野においてこれらのリスクに対処可能か検証。

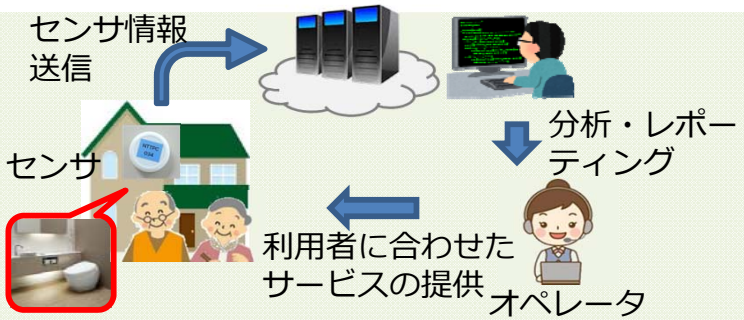
## 展開が期待されるサービス

### カーモビリティ分野

ロードサービス提供者が、各車両のセンサを通じて正確な情報を把握することにより、故障・事故の緊急時等にも迅速・的確に対応が可能となる。

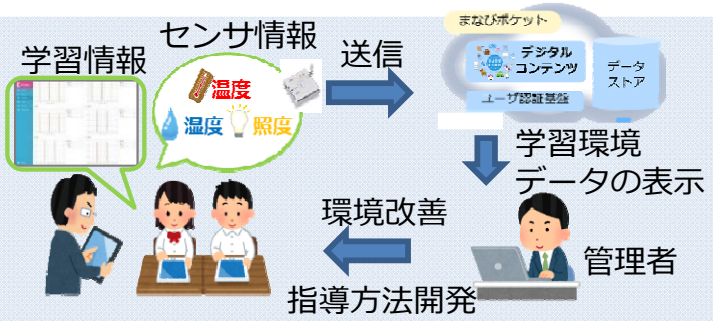

### スマートホーム分野

住宅内に設置された複数のセンサからのデータを通じて、居住者の健康状態等を推定し、必要な医療・健康サービスの提供が可能となる。




### エデュケーション分野

教室等に設置されたセンサから得られる温度・湿度等のデータと、生徒の学習情報・個人情報を組み合わせて分析することにより、よりよい学習環境の実現が可能となる。



# 実証実験の結果



○　**総じて通信の遅延やIoTセキュアゲートウェイを起因とするIoTサービスの停止等は発生せず、良好な運用が行えた**。IoTセキュアゲートウェイは認証、検知、対処といった機能は十分提供できており、**通信暗号化機能や秘匿性の高いデータ管理機能を有した堅牢なシステムである**ことも確認された。

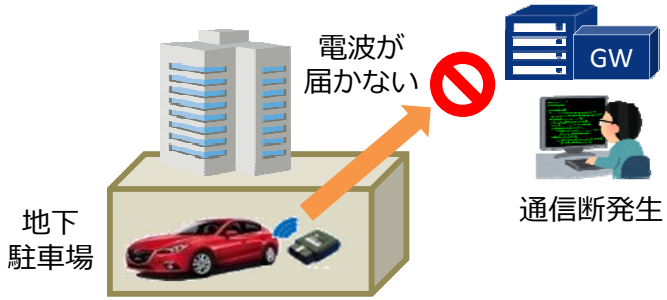
○　ただし、**IoTサービスの特性に基づく運用上の課題があり、**機能が十分に発揮できないケースがあった。その課題を解決するために、**異常な通信を検知する機能を向上させる必要がある**。

## 運用上の課題の例

カーモビリティ分野において、車両にIoT機器を取り付けるという特性上、地下駐車場に入り、**電波の届かない場所で通信が途絶えた場合**に以下の誤検知が発生。

・IoTセキュアゲートウェイがIoT機器の状態を把握できず、**盗難があったと誤検知**

・IoTセキュアゲートウェイがIoT機器との通信を再開した際に一気に送信されたデータを受信してしまい、**乗っ取りがあったと誤検知**



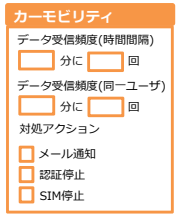

改善

## 検知機能の向上

### （１）機能改善

サービス提供者が利用シーンに応じて検知条件を設定することができるテンプレート（条件設定画面）を用意するといった機能改善が必要。

テンプレート無し




テンプレート利用

### （２）動的検知

サービス利用者の利用状況等の統計的なデータを収集・分析した結果に基づき、サービス利用者・IoT機器ごとに脅威検知に関する適正値を自動的に設定することが必要（※）。

※　AIを用いたデータ分析の活用も考えられる。

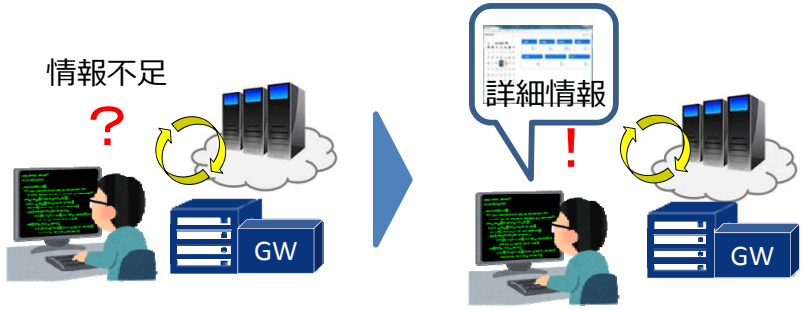
# IoTセキュアゲートウェイの普及に向けて必要な取組



○　実証実験で得られた課題を解決した上で、IoTセキュアゲートウェイの普及に向けて、**実用的なサービスモデルの提示の取組も必要**となる。

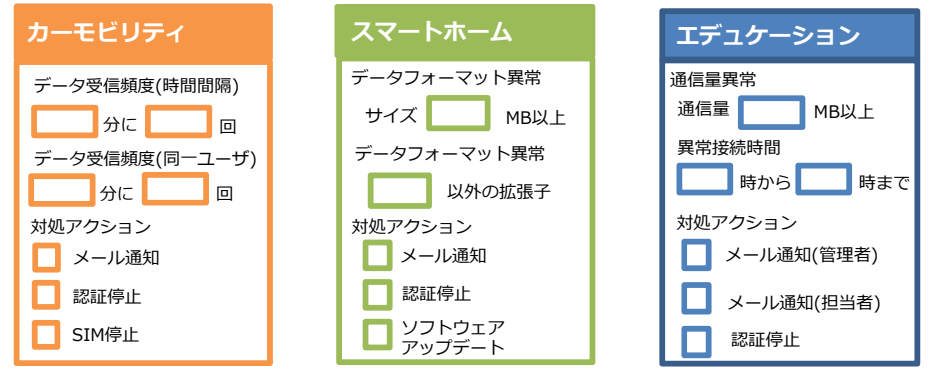
## （1）サービス提供者への詳細情報の提示

サービス提供者が迅速かつ適切な行動をとれるよう、サービス提供者に脅威検知のレベルや攻撃状況の詳細情報等を提示することが必要。




## （2）多様なテンプレートの作成

IoTセキュアゲートウェイを利用しやすくなるよう、各種IoTサービスに応じた多様なテンプレートの作成を行うことが必要。

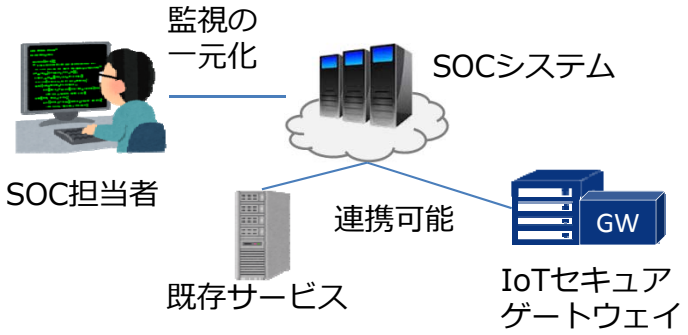



カーモビリティ分野　スマートホーム分野　エデュケーション分野

## （3）効率的なシステム運用環境の構築

効率的なシステム運用が行えるよう、SOC（※）のシステムとIoTセキュアゲートウェイの連携等が必要。

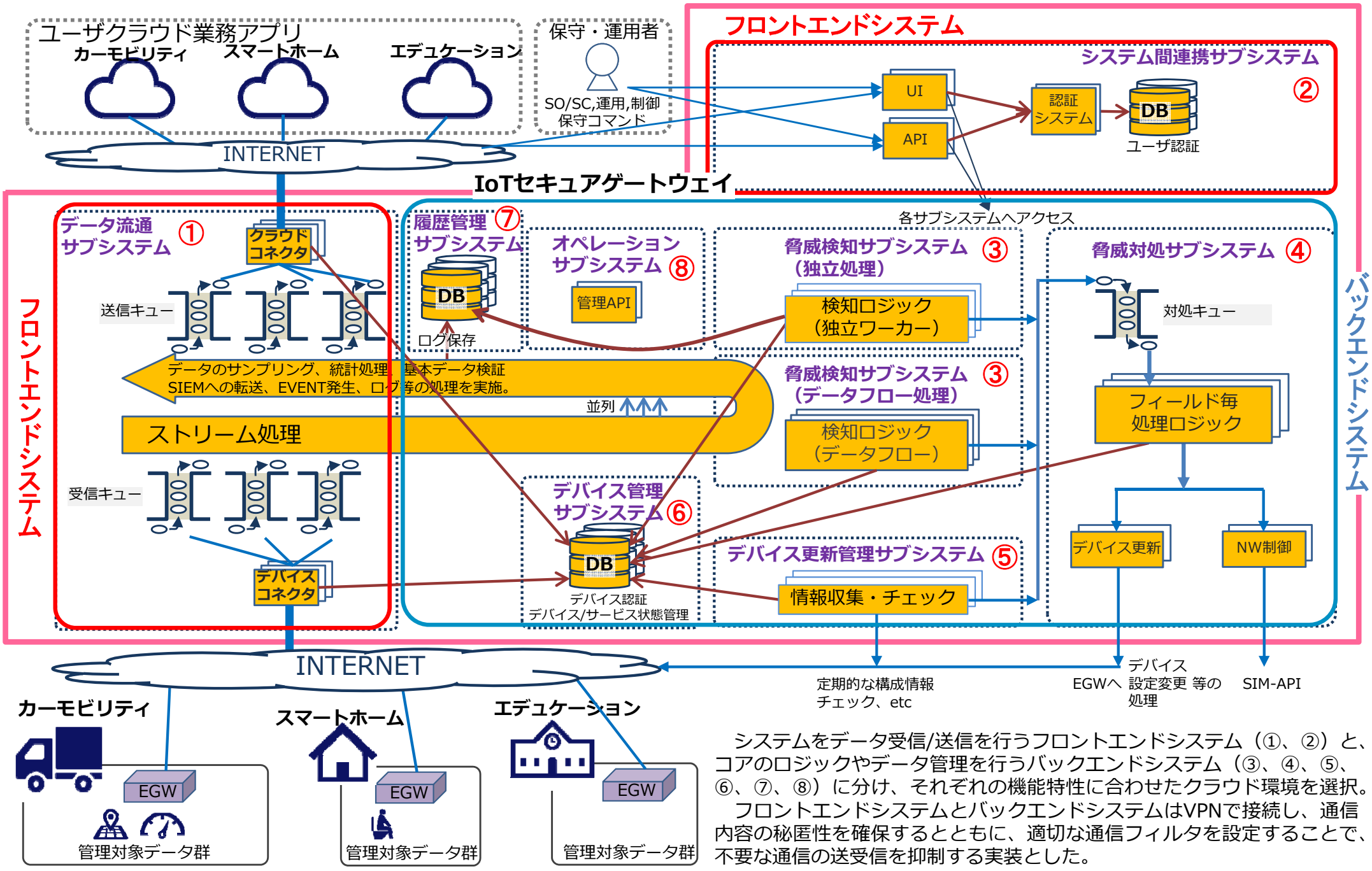
※　SOC：Security Operation Center



# 参考資料

# 実証実験におけるIoTセキュアゲートウェイの構成






システムをデータ受信/送信を行うフロントエンドシステム（①、②）と、コアのロジックやデータ管理を行うバックエンドシステム（③、④、⑤、⑥、⑦、⑧）に分け、それぞれの機能特性に合わせたクラウド環境を選択。

フロントエンドシステムとバックエンドシステムはVPNで接続し、通信内容の秘匿性を確保するとともに、適切な通信フィルタを設定することで、不要な通信の送受信を抑制する実装とした。

# 実証実験におけるIoTセキュアゲートウェイのサブシステム構成①



| No | サブシステム名 | 機能 | 説明 |
|---|---|---|---|
| ① | データ流通サブシステム | デバイス認証機能<br>（トークン認証） | デバイス管理サブシステムへ問い合わせ、初期又はトークン期限切れ時には共通認証ID、認証シークレット、ユニークIDの3要素認証でトークンとデバイス識別子の払い出しをする。実際のデータ受信時はトークンとデバイス識別子で認証をする。<br>・方式：トークン認証 |
| | | データ受信機能<br>（デバイスコネクタ） | デバイスからのHTTPSリクエストによりデータを受信する。受信後は、脅威検知サブシステムに受信したデータを渡す。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| | | データ送信機能<br>（クラウドコネクタ） | 脅威検知サブシステムから脅威検知ロジック適用後のデータ受け取り、クラウドへ送信する。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| | | データロギング機能 | 受信データのメタ情報を取得しデータベースに蓄積する。 |
| ② | システム間連携サブシステム | 管理者向けAPI・UI | フィールドの管理者に対し、IoTセキュアゲートウェイの持つ情報（デバイス情報等）を管理するためのブラウザGUIとAPIを提供する。APIのインターフェースは以下のとおり。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| | | 保守者向けAPI・UI | IoTセキュアゲートウェイの保守者に対し、システム全体の状態確認、コントロールを行うためのブラウザGUIとAPIを提供する。APIのインターフェースは以下のとおり。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| | | 認証機能 | 管理者・保守者が、API・UIを利用する際に、ID・PWにより認証する。 |
| ③ | 脅威検知サブシステム<br>（独立処理、データフロー処理） | データフロー検知機能 | データ流通サブシステムから受信データ受け取った受信データに対して、検知ロジック（スクリプトファイル）を適用し、脅威検知を行う。脅威か検知された場合、脅威対処サブシステムの対処キューに対処情報を登録する。 |
| | | 独立ワーカー検知機能 | 常駐的又は定期的に処理行い、必要なデータを収集し、検知ロジック（スクリプトファイル）を適用し、脅威検知を行う。脅威が検知された場合、脅威対処サブシステムの対処キューに対処情報を登録する。 |

# 実証実験におけるIoTセキュアゲートウェイのサブシステム構成②



| No | サブシステム名 | 機能 | 説明 |
|---|---|---|---|
| ④ | 脅威対処サブシステム | 脅威対処機能 | 対処キューより対処情報を取り出し、フィールドと脅威内容ごとの対処種別に紐付けられた対処ロジック（スクリプトファイル）を実行する。対処の内容は以下の三つである。<br>・IoTセキュアゲートウェイ内部での対処（デバイス管理サブシステムでのデバイスの認証無効化）<br>・NWの停止（デバイスのモバイルSIMの停止）<br>・デバイスの更新（デバイス更新サブシステムの監査の結果に基づくデバイスの設定等の更新） |
| ⑤ | デバイス更新管理サブシステム | デバイス監査機能 | 定期的にデバイス管理サブシステムへ問合せを行い、監査対象デバイスを抽出し、フィールド・デバイスごとに用意された監査ロジック（スクリプトファイル）を実行する。監査の結果、異常と判断された場合は、脅威対処サブシステムの対処キューに対処情報を登録する。 |
| ⑥ | デバイス管理サブシステム | 認証機能 | 初期又はトークン期限切れ時には共通認証ID、認証シークレット、ユニークIDの3要素認証からトークンとデバイス識別子の払い出しをする。実際のデータ受信時はトークンとデバイス識別子で認証をする。<br>・方式：トークン認証 |
| | | デバイス管理機能 | デバイスを管理するAPIを持つ。IoTセキュアゲートウェイ内の他のサブシステムから参照される。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| ⑦ | 履歴管理サブシステム | 履歴管理機能 | IoTセキュアゲートウェイを通る送信・受信データの履歴、登録デバイス状態履歴、脅威検知・対処履歴、定期監査履歴を管理する。IoTセキュアゲートウェイ内各サブシステムに対し、登録・検索APIの提供を行う。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |
| ⑧ | オペレーションサブシステム | システム管理オペレーション機能 | IoTセキュアゲートウェイを構成する各サブシステムの動作状況の確認やスケール変更などのシステムの保守者に対するオペレーションを行うためのAPIを持つ。<br>・プロトコル：HTTPS<br>・データ形式：JSON形式 |

# 実証実験で用いたIoT機器



実証実験では次の条件を満たすIoT機器を用いた。

- Wi-Fi、Bluetooth、LTE、3G等において、通信が可能であること。
- 認証を行うための情報群を有していること。または、後からその仕組みを付与できること。
- 時間単位、日単位等、様々な頻度で通信が可能であること。

## カーモビリティ分野


【GX4xONC OBDⅡ】

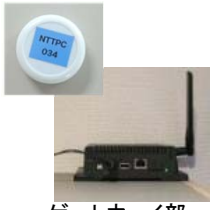
| | |
|---|---|
| 識別情報 | 個体識別情報（IMEI番号） |
| 通信形態 | SIMによるインターネットへの通信（3G） |
| 通信頻度 | エンジン起動時は5分ごとにデータ送信<br>エンジン停止時は6時間ごとにデータ送信 |

## スマートホーム分野

【試作機】

| | |
|---|---|
| 識別情報 | 個体識別情報（MACアドレス・基盤シリアル） |
| 通信形態 | ・SIMによるインターネットへの通信（LTE）<br>・Wi-Fiで無線LANアクセスポイントに接続<br>・アクセスポイントから光ファイバーによりインターネットへの通信 |
| 通信頻度 | 稼働状態において、利用の都度データ送信 |

センサー部



ゲートウェイ部

【試作機】

| | |
|---|---|
| 識別情報 | 個体識別情報（MACアドレス） |
| 通信形態 | ・センサ部からBLE（Bluetooth Low Energy）により、宅内のゲートウェイ部にデータ送信<br>・ゲートウェイ部内蔵のSIMによるインターネットへの通信（3G） |
| 通信頻度 | 稼働状態において、検知の都度データ送信 |

## エデュケーション分野

センサー部

ゲートウェイ部

【センサー部：温・湿・照度ノード（SW-4210-1204）】
【ゲートウェイ部：Armadillo-IoTゲートウェイ G3】

| | |
|---|---|
| 識別情報 | 個体識別情報（ID） |
| 通信形態 | ・センサ部から920MH z (独自プロトコル)の無線通信で、ゲートウェイ部にデータ送信<br>・ゲートウェイ部内蔵のSIMで通信（3G） |
| 通信頻度 | 稼働状態において、5分ごとにデータ送信 |

【Chromebook R11】

| | |
|---|---|
| 識別情報 | 個体識別情報（ユーザID） |
| 通信形態 | ・Wi-Fiで無線LANアクセスポイントに接続<br>・アクセスポイントから光ファイバーによりインターネットへの通信 |
| 通信頻度 | 稼働状態において、不定間隔でデータ送信 |

# 実証実験の実施内容①



| 検証分類 | 検証名 | 実施概要・観点 | 結果 | | | 想定リスク |
|---|---|---|---|---|---|---|
| | | | カーモビリティ | スマートホーム | エデュケーション | |
| IoTデバイスの認証 | 個体識別情報、グループ属性情報、パスワードを用いた認証方式の検証 | 事前に登録されている情報を用いて認証要求を送信し、IoTセキュアゲートウェイが認証要求に対して認証が成功することを確認 | ○ | ○ | ○ | 不正アクセス |
| | | 事前に登録されていない情報を用いて認証要求を送信し、IoTセキュアゲートウェイが認証要求に対して認証が失敗することを確認 | ○ | ○ | ○ | |
| | 認証されたIoTデバイスに対する通信許可方式の検証 | 認証済みのデバイスのアクセスが許可されることを確認 | ○ | ○ | ○ | |
| | 認証されないデバイスに対する通信遮断方式の検証 | 認証を得ていないデバイスのアクセスを拒否することを確認 | ○ | ○ | ○ | |
| IoTデバイスからの通信に関する暗号化 | 通信電文の暗号化方式に関する検証 | デバイスの通信を盗聴（デバイス上でパケットをキャプチャ）し、通信が暗号化されていることを確認 | ○ | ○ | ○ | 盗聴 |
| IoTデバイスに関する情報管理 | デバイス個体情報の管理に関する検証 | IoTセキュアゲートウェイの管理機能から新規デバイスの登録、既存デバイスの削除ができることを確認 | ○ | ○ | ○ | 不正アクセス<br>乗っ取り |
| | | 事前に登録されていない情報を用いて認証要求を送信し、IoTセキュアゲートウェイが認証要求に対して認証が失敗することを確認 | ○ | | ○ | |
| | デバイスより収集した情報の管理に関する検証 | IoTセキュアゲートウェイで受信したデータがSSLにより暗号化されていることを確認 | ○ | ○ | ○ | |
| | | HTTPのリクエストを拒否することを確認 | ○ | ○ | ○ | |
| | デバイス通信ログの管理に関する検証 | データベースのデータファイルから関連情報が読めないことを確認 | ○ | ○ | ○ | |
| | | コピーデータベースでクエリを行ってもエラーになることを確認 | ○ | ○ | ○ | |
| IoTデバイスの状態や挙動に関する分析 | データ受信頻度による異常検知の検証 | エンジン停止時の通常通信（６時間に１回）より多い頻度（６時間に1回より多くの頻度)で通信が行われた場合、異常を検知することを確認 | △<br>※１ | | | 乗っ取り |
| | | エンジン起動時の通常通信（５分に１回）より多い頻度（５分に１回より多くの頻度）で通信が行われた場合、異常を検知することを確認 | △<br>※１ | | | 乗っ取り |
| | | デバイスからの通信がない場合（６時間通信がない場合）、異常を検知することを確認（IoTセキュアゲートウェイに登録済みのデバイスを車両から取り外すことにより実施する。） | △<br>※１ | | | 盗難 |
| | | デバイスを外部に持ち出しセンサ情報が送信されなくなった場合に、異常を検知することを確認（盗難の可能性の注意喚起として、通常（５分に１回）よりも少ない頻度の送信になったことも検知) | | | ○ | 盗難 |
| | | 同一ユーザで異常な頻度（１分以内に10回以上）の認証要求を行い、異常を検知することを確認 | | | ○ | 不正アクセス |
| | | 異常な時間（22時～翌６時）に認証が成功し、異常を検知することを確認 | | | ○ | 不正アクセス |
| | タイムスタンプによる異常検知の検証 | タイムスタンプが異常なセンサ情報を送信し、異常を検知することを確認 | | ○ | ○ | 乗っ取り |

※１　車両に設置されたIoT機器の特性上、地下駐車場など電波の届かない場所において、送信されるべきデータが送信されず、通信を検知できないことがあった。また、その後通信状況が改善され、保存されていたデータが短い間隔で連続して送信されることにより、閾値を超えたデータ送信頻度となり、脅威として誤検知されることがあった。

# 実証実験の実施内容②



| 検証分類 | 検証名 | 実施概要・観点 | 結果 | | | 想定リスク |
|---|---|---|---|---|---|---|
| | | | カーモビリティ | スマートホーム | エデュケーション | |
| IoTデバイスの状態や挙動に関する分析 | 通信量による異常検知の検証 | SIMの通信量とデバイスからIoTセキュアゲートウェイへの通信量が大幅に異なっている場合、異常を検知することを確認 | △<br>※2 | | △<br>※3 | 乗っ取り |
| | データ送信元による異常検知の検証 | SIMのグローバルIPアドレスとは異なる送信元IPアドレスからセンサ情報を送信し、異常を検知することを確認 | ○ | ○ | ○ | なりすまし |
| | | 同一送信元IPアドレスから複数デバイスの情報を送信し、異常を検知することを確認 | ○ | | | なりすまし |
| | | 実証実験のネットワーク以外のネットワークから接続をしてデバイス認証を行い、異常を検知することを確認 | | ○ | △<br>※4 | 盗難 |
| | データフォーマットによる異常検知の検証 | データサイズがあらかじめ定めたデータサイズの上限以上のデータを送信し、異常を検知することを確認 | ○ | ○ | ○ | 乗っ取り<br>（カーモビリティのみ「なりすまし」） |
| | | データが途中で欠落した形（正しいJSONフォーマットでない）データを送信し、異常を検知することを確認 | | ○ | | 乗っ取り |
| 異常時における原因の特定と対策 | 認証機能によるデバイス通信無効化の検証 | デバイスの状態が異常なデバイスからのアクセスを認証機能により不許可となることを確認 | ○ | ○ | ○ | 盗難、<br>乗っ取り |
| | SIMによるデバイス通信無効化の検証 | 異常が検知されたデバイスのSIMを停止できることを確認 | ○ | ○ | ○ | 盗難、<br>乗っ取り |
| | デバイス内ソフトウェアの設定変更・更新の検証 | ソフトウェアの設定ファイルを改変することで、デバイスの管理情報が不一致になり、異常が検知されたデバイスについて、管理者へ通知する機能をIoTセキュアゲートウェイが提供できることを確認 | | ○ | | 乗っ取り |
| | | 正常運用で使用しないプロセス（不正プロセス）を実行することで異常が検知され、管理者へ連絡できることを確認 | | | ○ | 乗っ取り |
| | デバイス内情報の収集・解析の検証 | 異常が検知されたデバイスについて、IoTセキュアゲートウェイが管理者に登録されている情報（デバイス内情報など）を提供できることを確認 | | △<br>※5 | | 乗っ取り |
| 脅威の特定と対策 | デバイス構成管理の検証 | ソフトウェアのバージョンを正常でないバージョンにダウングレードされた場合に異常が検知され、管理者へ連絡できることを確認 | | ○ | ○ | 乗っ取り |
| | デバイス内ソフトウェア更新の検証 | ソフトウェアの脆弱性が発見された場合などに、ハッシュ値を更新することで一括してソフトウェアの更新ができることを確認 | | ○ | ○ | 乗っ取り |

※2　データ送信失敗時にリトライを繰り返すため、リトライしたデータはSIMの通信量としてはカウントされるが、デバイスからIoTセキュアゲートウェイへの通信量としてはカウントされず、通信量の不一致が起き、脅威として誤検知されることがあった。

※3　デバイス-IoTセキュアゲートウェイ外の通信（インターネット側からデバイスへの予期しない通信）が発生したため、閾値を超える通信量となり、脅威として誤検知されることがあった。

※4　児童が指定されたデバイス以外を用いて実証実験のネットワーク（学校のWi-Fi環境）以外から接続した場合に、脅威として誤検知されることがあった。

※5　IoTセキュアゲートウェイに登録されている情報に基づいて不正なプロセスのチェックを行ったため、IoTセキュアゲートウェイに登録されていない正常なプロセスを起動した際に脅威として誤検知されることがあった。