# IOTセキュリティ・ガイドライン

## 概要説明書


# IoT セキュリティ・ガイドライン概要説明書

## バージョン 2.0

## 2017 年 10 月 31 日

*本文書は GSMA の拘束力のない恒久参照文書です。*

### セキュリティ区分：公開可能

本文書の入手および配布は、セキュリティ区分で認められた者に限られます。本文書は GSM の機密文書であり、著作権保護が適用されます。本文書はその提供目的のためにのみ使用されるものとし、本文書の全部もしくは一部の情報を、GSM の書面による事前の承認なくセキュリティ区分によって認められている者以外に開示する、またはそれ以外の方法で利用可能にすることを禁じます。

# 目次

# 1 はじめに

## 1.1 概要

モノのインターネット（IoT）の登場を受けて、新たに革新的な接続機能を備えた製品やサービスを開発しようとするサービス提供者が誕生しています。アナリストたちは、今後 10 年で数十万もの新しい IoT サービスが登場し、何十億もの新たな IoT デバイスが接続つながるようになると予測しています。新たなエコシステムのすべての関係者にとって、このようなモノのインターネットの急成長は、サービス提供を拡大させ、顧客基盤を増強するための大きなチャンスとなっています。

アナリストたちは、数多くの新たな IoT サービスの展開に伴い、セキュリティの問題が大きな課題になるとともに、絶えず拡大する種類豊富な IoT サービスに広域の接続性が提供されることによって、エコシステム全体が不正と攻撃にさらされるリスクが増大することを指摘しています。この分野に攻撃者が関心を寄せ始めていることを示す証拠はすでにたくさんあります。

IoT 関連の新サービスの提供者が、特定の市場セグメントを対象として革新的な新サービスを開発するにあたり、サービスに対する潜在的な脅威を認識していない恐れがあります。場合によっては、サービス提供者が通信回線やインターネットへの接続サービスを事前に準備していなかったり、デバイス内でのインターネット接続の確立によって生じるリスクを軽減するためのスキルと専門知識を利用できる体制を整えていなかったりする場合があります。一方、攻撃者は技術とセキュリティの脆弱性を熟知しており、脆弱性が発覚すればすぐに悪用しようとするでしょう。デバイスのセキュリティ侵害を引き起こした攻撃は数多く存在します。セキュリティ侵害を受けたデバイスはデータを流出させたり、他のデバイスを攻撃したり、関連するサービスや無関係のサービスに対して障害を引き起こしたりする可能性があります。

自動車、医療、家電製品、地方自治体等のセクターに属するサービス提供者の多くは、自分たちの市場固有のセキュリティ要件が必要であると考えている場合がありますが、これは概して正しくありません。ほぼすべての IoT サービスは、他の多くの通信、計算および IT のソリューションに類似する技術を利用したエンドポイントデバイスとサービスプラットフォームのコンポーネントを用いて構築されています。また、攻撃者の動機や、セキュリティ侵害が成功した場合の影響は様々であるにもかかわらず、これらのサービスが直面する脅威とそれを緩和するための考えられるソリューションは一般的に非常に類似しています。

GSMA がけん引する通信業界には、顧客に安全性の高い製品とサービスを提供してきた長い歴史があります。安全な製品やサービスの提供はこの業界にとって目標でもあり、目標を達成するためのプロセスでもあるのです。ソリューションがセキュリティの脅威に対応することを保証するためには、徹底した警戒体制、イノベーション、迅速な対応、継続的な改善が求められます。

新たに市場に投入される IoT サービスの安全性を確保するために、ネットワーク事業者はネットワーク、サービスおよびデバイス装置関連の事業者とともに、セキュリティに関する専

門知識を、IoT サービスを開発しようとしているサービス提供者と共有することを望んでいます。

そこで GSMA は、新たな IoT サービスを開発しようとしているサービス提供者向けに、このセキュリティ・ガイドラインを作成しました。

## 1.2 GSMA IoT セキュリティ・ガイドライン文書群

本文書は、黎明期の「モノのインターネット」業界における IoT のセキュリティ問題に対する共通の理解を確立する一助となることを目的とした、GSMA による一連のセキュリティ・ガイドライン文書の導入部にあたります。この一連のガイドライン文書は、サービスのライフサイクル全体を通じてセキュリティのベストプラクティスが実装されることを保証にするために、安全性の高い IoT サービスを開発するための方法論を示すもので、IoT サービスにおける一般的なセキュリティへの脅威と脆弱性を軽減する方法についての推奨事項を提示しています。

以下の図は、GSMA セキュリティ・ガイドライン文書群の構成を示しています。本文書（本概要説明書）を手引きとして参照した後に、その他の関係文書へと読み進めることをお勧めします。

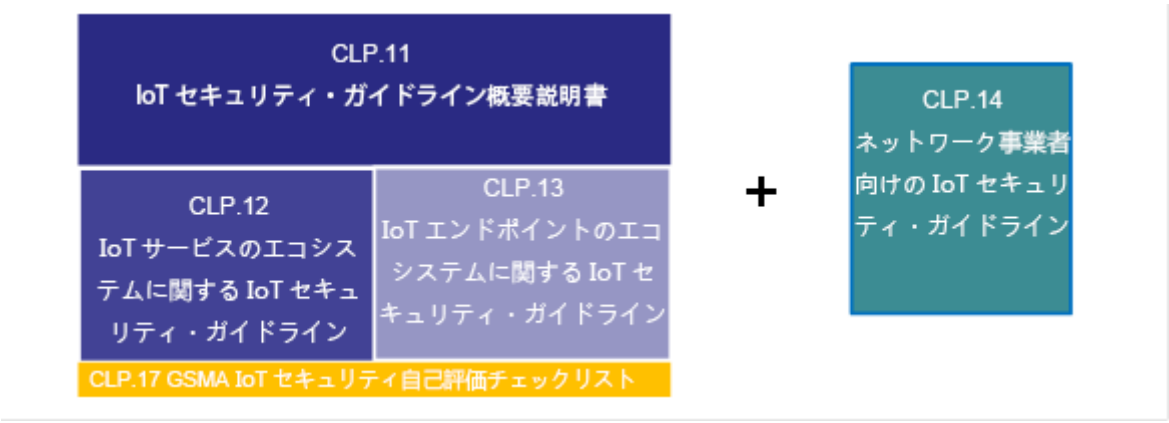


**図 1 - 「GSMA IoT セキュリティ・ガイドライン」文書の構成**

IoT エコシステムで活動するネットワーク事業者、IoT サービス提供者およびその他の関連事業者の皆様には、GSMA 文書 CLP.14「ネットワーク事業者のための IoT セキュリティガイドライン」[13]を参照することをお勧めします。同文書は、IoT サービス提供者にサービスを提供しようとしているネットワーク事業者向けに、システムのセキュリティやデータのプライバシーを保証するための最高水準のセキュリティ・ガイドラインを提示しています。

### 1.2.1 GSMA IoT セキュリティ評価チェックリスト

GSMA 文書 CLP.17 [16]には、評価チェックリストが添付されています。IoT 製品、サービスおよびコンポーネントのサプライヤーは、同チェックリストを使用して自社の製品、サービスおよびコンポーネントが「GSMA IoT セキュリティ・ガイドライン」を遵守しているかどうかを自己評価することができます。

「GSMA IoT セキュリティ評価チェックリスト」[16]に評価を記入することで、サプライヤーはサイバーセキュリティーのリスクから自社の製品、サービスおよびコンポーネントを守るために講じているセキュリティ対策を実証することができます。

同チェックリストへの回答は、記入したチェックリストを GSMA に提出することで完了することができます。チェックリストへの回答手順については、GSMA 公式ウェブサイトを参照してください。

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

## 1.3 文書の目的

IoT セキュリティ・ガイドライン文書群は、IoT 関連の技術またはサービスの実装者に対して、安全性の高い製品の確立に向けた一連の設計ガイドラインを提示することを目的としています。この目的のために、本文書は技術またはサービスのどの側面が実装者に関連するかを説明する、包括的なモデルの役割を果たします。これらの側面またはコンポーネントを特定することにより、実装者は各コンポーネントに関連するリスクを評価し、その補償方法を決定することができます。また、それぞれのコンポーネントを *サブコンポーネント*に分類し、リスクをより詳細に記述することもできます。これにより、実装者は攻撃のコスト、是正コスト、そしてリスクに対処しなかった場合のコストを仮算定でき、リスクごとに優先順位を付けることが可能となります。

本文書の適用範囲は、IoT サービスの設計と実装に関する推奨事項に限定されます。

本文書は、新たな IoT 仕様や標準の作成を促すことを意図したものではなく、現時点で利用可能なソリューション、標準、ベストプラクティスを示すものです。

本文書には、既存の IoT サービスの陳腐化を加速させる意図はありません。

特定の地域の国内法令および規則を遵守することによって、本文書のガイドラインが無効となる場合がありますのでご注意ください。

## 1.4 想定読者

本文書が想定する主な読者は次の通りです。

- IoT サービス提供者 - 新たに革新的な接続機能を備えた新製品やサービスを開発しようとしている企業または組織。IoT サービス提供者が活動する分野の一例には、スマートホーム、スマートシティー、自動車、輸送、医療、公益事業、家電製品が含まれます。
- IoT デバイス製造業者 - IoT サービス提供者向けに IoT サービス対応の IoT デバイスを提供する業者。
- IoT 開発業者 - IoT サービス提供者向けに IoT サービスの構築を代行する業者。
- ネットワーク通信事業者 - 自社が IoT サービス提供者であるか、または IoT サービス提供者向けに IoT サービスの構築を代行する業者。

## 1.5 用語の定義

| 用語 | 説明 |
|---|---|
| アクセスポイント名 | エンドポイントデバイスを取り付けるネットワーク接続ポイントの識別子。異なるサービス種類ごとに決められており、多くの場合、ネットワーク事業者別に設定される。 |
| 攻撃者 | 一般的に情報の取得、破壊、制限または改ざんを目的とした、IoT サービスに悪質な脅威を与える者。ハッカー、脅威エージェント、脅威アクター、詐欺師など。脅威の発生源として、個々の犯人、組織犯罪、テロ、敵対国およびその代理人、産業スパイ、ハッカー集団、政治活動家、マニアハッカー、研究者、さらには意図的でないセキュリティとプライバシーの侵害などが考えられる。 |
| クラウド | アプリケーションおよびデータのホスト、保存、管理および処理を行う、インターネット上にあるリモートサーバーのネットワーク。 |
| 複合エンドポイント | 長距離通信リンク（移動体通信、衛星、イーサネット等の配線接続など）において、バックエンドのサーバーへの継続的な接続性を備えたエンドポイント・モデルの一種。詳細については、CLP.13 [4]を参照。 |
| コンポーネント | 文書 CLP.12 [3]および CLP.1 3 [4]に記載されているコンポーネントの説明を参照。 |
| 埋め込み SIM | デバイス内での取り外しや交換を意図せず、GSMA SGP.01 [2]に従ったプロファイルで安全性の高い変更が可能な SIM。 |
| エンドポイント | 軽量エンドポイント、複合エンドポイント、ゲートウェイまたはその他の接続機能を備えたデバイスの総称。詳細については、CLP.13 [4]を参照。 |
| エンドポイントのエコシステム | 斬新な方法で現実世界をデジタル世界につなぐ、複雑性の低いデバイス、リッチデバイス、ゲートウェイからなる構成。詳細については、セクション 4.2 を参照。 |
| モノのインターネット | モノのインターネット（IoT）とは、複数のネットワークを通じてインターネットに接続された様々なマシン、デバイス、器具が連動して動作することを指す。これらのデバイスには、タブレットや家電製品などの日用品のほか、データの送受信ができる通信機能を備えた車両、モニター、センサーなどのマシンが含まれる。 |
| IoT サービス | サービスを実行するために IoT デバイスからのデータを利用するコンピューターププログラム。 |
| IoT サービス提供者 | 新たに革新的な接続機能を備えた製品やサービスを開発しようとしている企業または組織。 |
| ネットワーク事業者 | IoT エンドポイントデバイスを IoT サービスのエコシステムに接続する、通信回線の運営者および所有者。 |
| 組織の信頼の基点（Root of Trust） | ID、アプリケーション、通信のセキュリティを暗号によっていかにして確保できるか（確保すべきか）を定める、一連の暗号化ポリシーおよび手順。 |
| 推奨事項 | 文書 CLP.12 [3]および CLP.1 3 [4]に記載されている推奨事項の説明を参照。 |
| リスク | 文書 CLP.12 [3]および CLP.1 3 [4]に記載されているリスクの説明を参照。 |

| 用語 | 説明 |
|---|---|
| セキュリティタスク | 文書 CLP.12 [3]および CLP.1 3 [4]に記載されているセキュリティタスクの説明を参照。 |
| サービスのアクセスポイント | 通信回線を経由した、IoT サービスのバックエンドにあるインフラストラクチャへのエントリーポイント。 |
| IoT サービスのエコシステム | フィールドで展開するエンドポイントに機能を提供し、そこからデータを収集するために必要な一連のサービス、プラットフォーム、プロトコルおよびその他の技術。詳細については、セクション 3.1 を参照。 |
| 加入者識別モジュール（SIM） | モバイルネットワークとネットワークサービスへのアクセス時に、デバイス認証のためにモバイルネットワークが使用するスマートカード。 |
| UICC | ETSI TS 102 221（欧州電気通信標準化機構の技術仕様）に規定されている、暗号が異なるセキュリティドメインにおいて複数の標準化されたネットワークまたはサービスの認証アプリケーションをサポートすることができる、セキュアエレメントのプラットフォーム。ETSI TS 102 671 に規定されている埋め込み式要素に埋め込まれることがある。 |

## 1.6 略語

| 用語 | 説明 |
|---|---|
| 3GPP | 第 3 世代プロジェクト・パートナーシップ |
| API | アプリケーション・プログラム・インターフェイス |
| APN | アクセスポイント名 |
| CERT | コンピューター緊急対処チーム |
| CLP | GSMA のコネクテッド・リビング・プログラム |
| CPU | 中央処理装置 |
| EAP | 拡張認証プロトコル |
| EEPROM | 電気的に消去可能なプログラマブル読み取り専用メモリ |
| GBA | 汎用ブートストラッピング・アーキテクチャ |
| GPS | グローバル・ポジショニング・システム |
| GSMA | GSM Association |
| GUI | グラフィック・ユーザー・インターフェイス |
| HIPAA | 医療保険の相互運用性と説明責任に関する法令 |
| IoT | モノのインターネット |
| LPWA | ローパワー・ワイドエリア |
| LTE-M | マシン向けロング・ターム・エボリューション |
| NB-IoT | 狭帯域モノのインターネット |
| NIST | 国立標準技術研究所 |
| OBD | 自己診断機能 |
| OCTAVE | 運用上重要な脅威、資産および脆弱性評価 |

| 用語 | 説明 |
|---|---|
| OMA | オープン・モバイル・アライアンス |
| PIA | プライバシー影響評価 |
| PII | 個人識別情報 |
| RAM | ランダム・アクセス・メモリ |
| SIM | 加入者識別モジュール |

## 1.7 参考文献

| 参照 | 文書番号 | タイトル |
|---|---|---|
| [1] | 該当なし | “The Mobile Economy 2017” http://www.gsmamobileeconomy.com/ |
| [2] | SGP.01 | “Embedded SIM Remote Provisioning Architecture” https://www.gsma.com/iot/embedded-sim/ |
| [3] | CLP.12 | IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |
| [4] | CLP.13 | IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |
| [5] | 該当なし | NIST Risk Management Framework http://csrc.nist.gov/groups/SMA/fisma/framework.html |
| [6] | CMU/SEI-2007-TR-012 | Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process http://www.cert.org/resilience/products-services/octave/ |
| [7] | 未使用 | 未使用 |
| [8] | TS 33.220 | Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org |
| [9] | RFC 4186 | Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) www.ietf.org |
| [10] | 該当なし | Conducting privacy impact assessments code of practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf |
| [11] | 該当なし | Open Mobile Alliance http://openmobilealliance.org/ |
| [12] | 該当なし | oneM2M Specifications http://www.onem2m.org/ |
| [13] | CLP.14 | IoT Security Guidelines for Network Operators https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |
| [14] | GE.11-13201 | Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* |

| 参照 | 文書番号 | タイトル |
|---|---|---|
| | | www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf |
| [15] | 該当なし | Right to Internet Access<br>https://en.wikipedia.org/wiki/Right_to_Internet_access |
| [16] | CLP.17 | GSMA IoT Security Assessment Checklist<br>https://www.gsma.com/iot/iot-security-assessment/ |

# 2 モノのインターネットがもたらす課題

数年前に国連が公表した特別報告書において、インターネットを基本的人権とみなし、世界中のすべての人がブロードバンドのサービスを利用できるようにすべきであるとの提言がなされました[14]。最近では、インターネットへのアクセスが広く利用できることを保証し、国民が情報とインターネットを利用する機会を国が正当な理由なく制限することを防止する法律が、フランス、ギリシャ、スペインをはじめとする国々で採択されています[15]。

これらの動きは、インターネットの発展による急速な社会的および技術的変化を受けて生じたものです。その結果、インターネットは日常に当たり前に存在し、あらゆる情報の主な情報源の 1 つでありながら、愛する家族や友人とつながっているための最も一般的な方法となりました。インターネットは単なる技術ではなく、私たちの*一部*となっています。

接続性の維持に対する要求の高まりに伴い、ここ数年間で技術が爆発的に発展しました。「モノのインターネットの時代がやってきた」と技術者は 10 年前から主張していたものの、5 年前までは、情報へのユビキタス・アクセスに対する関心とそれに必要なコストモデルが上手く融合し、実用的なビジネスモデルに結実することはありませんでした。ところがここに来てコンポーネントのコストが急激に低下し、無線サービスへのアクセスとアクセス速度が劇的に改善したのです。情報と接続性に対して社会の要求は高まる一方であることから、プロトコル、バッテリー寿命、さらにはビジネスモデルまでもが進化を遂げました。

つまり、これこそが「モノのインターネット」なのです。IIoT とは実際のところ、モノではなく社会に係わる現象、つまり「社会のインターネット」といえるでしょう。この新たな生活様式では、私たち人間の経験とデジタルの経験は個別に存在するものではなくなり、ますます結びつきが強くなっています。

そして、人間の身体的な経験が今まで以上にデジタル世界につながり、デジタルのセキュリティが現実世界にこれまで以上に直接的な影響を及ぼすようになった今、セキュリティ保護の必要性が増大しています。モノのインターネットは、知識のデータベースや共有経験をより一層充実させ、イノベーションの爆発をもたらすという目標に向けて、全世界の人々が共に前進するための素晴らしい機会です。しかし、それが効果を発揮するためには、接続性をもたらす技術のセキュリティを保護し、プライバシーや信頼性、サービスの質を強化しなくてはなりません。優れた実用品であり、不可欠かつ基本的な必需品でもある IoT を、それを必要とするすべての人にとって常時利用可能なものにするためには、このような強化が必要なのです。

モノのインターネットを真に発展させるためには、その成長過程において避けられないセキュリティに関する次の問題を解決する必要があります。

- 可用性：エンドポイントと各サービスとの常時接続を確保する
- ID：エンドポイントやサービス、顧客、エンドユーザーが操作するエンドポイントを認証する
- プライバシー：個々のエンドユーザーに被害が及ぶリスクを軽減する
- セキュリティ：システムの完全性を確認および追跡し、確実にモニタリングする

## 2.1 可用性に関する課題

モノのインターネットが期待されるペースで発展するためには、エンドポイントデバイスがお互いに、そしてエンドユーザーやバックエンドのサービスと、常時情報を交換できなくてはなりません。これを実現するためには、低消費電力デバイスに対する持続的な接続を可能にする新技術（NB-IoT、LTE-M など）を展開する必要があります。この問題は、現代社会に対するユビキタスなインターネットアクセスの課題にぴったりと一致します。この可用性に関する課題を克服するには、以下の問いに対する答えを明らかにしなくてはなりません。

- 従来のセルラーシステムと同程度のセキュリティ水準で、いかにしてローパワー・ワイドエリア（LPWA）ネットワーク（NB-IoT、LTE-M など）を展開および運用することができるか。
- IoT エンドポイントがネットワークの境界をまたいで移動する場合、複数の移動体通信事業者で同水準のセキュリティを確保するにはどうすればよいか。
- 通信をゲートウェイのエンドポイントに依拠するキャピラリーネットワークのエンドポイントまでネットワーク信頼性を*転送*するにはどうすればよいか。
- 安全性の高い通信環境で軽量エンドポイントの電力制限に対応するにはどうすれはよいか。

## 2.2 ID に関する課題

IoT 製品またはサービスのエコシステムの内部でエンドポイントを作動させるには、ピアとサービスがエンドポイントを確実に識別できる必要があります。この IoT 技術の重大かつ基本的な性質によって、サービスとピアによるデータの配信先の保証が確保されます。ID に直接関連する問題は、情報とサービスへのアクセスだけではありません。以下の点についても検討する必要があります。

- エンドポイントを操作するユーザーとエンドポイントの ID を強く関連付けることは可能か。
- サービスとピアは、エンドポイントの ID を確認することによって、どのようにエンドユーザーの ID を確認できるのか。
- エンドポイントのセキュリティ技術による、ピアとサービスの安全な認証は可能か。
- 認証済みのサービスとピアを、不正なサービスとピアがなりすますことは可能か。
- デバイスの ID をいかにして不正操作や改ざんから守るか。
- エンドポイントとネットワークは、どのようにして IoT サービスによるエンドポイントへのアクセスを許可することを保証するか。

## 2.3 プライバシーに関する課題

プライバシーを既存の製品やサービスに対するアドオンとみなすことは、もはや不可能です。現実世界はデジタル世界での動作に直接影響されるため、最初の段階から製品の中にプライバシーを構築し、すべての動作が認証を受け、すべての ID が確認されるようにしつつ、動作とそれに関連するメタデータが権限のないユーザーにさらされることのないよう保証しなくてはなりません。これは、製品やサービスに対して適切なアーキテクチャを定義することによってのみ可能となり、遡及的に行うのは非常に困難で費用もかかります。

医療機器、自動車関連のソリューション、産業用制御システム、ホームオートメーション、建物セキュリティシステムなどはすべて、現実世界における人間の生活に直接的な影響を及ぼします。プライバシーに関するデータの流出、そして身体に対する潜在的な危害を低減するために、これらの製品やサービスに対する最高水準の保証を確保することが、エンジニアの責務となります。

そのため、プライバシーがエンドユーザーにいかに影響するかだけでなく、次のような IoT 技術の設計方法についても検討する必要があります。

- エンドポイントの ID が、権限のないユーザーにさらされていないか。
- エンドポイントや IoT サービスの固有の識別子によって、エンドユーザーやエンドポイントが物理的に監視または追跡される恐れはないか。
- エンドポイントや IoT サービスから収集されるデータが、エンドユーザーの物理的属性（位置、動作、*スリープ*中か*起動中*かなどの状態）を示唆したり、それに直接関連付けられてないか。
- 生成された暗号文のパターンを読み取られないようにするために、万全なセキュリティに機密性と完全性が確保されているか。
- 製品やサービスは、ユーザー固有の個人識別情報（PII）をどのように保存または処理するか。
- エンドユーザーは、IoT サービスや製品でストレージを管理したり、PII を利用したりできるか。
- データを保護するために使用されるセキュリティキーやセキュリティ・アルゴリズムは、リフレッシュできるか。

## 2.4 セキュリティに関する課題

インターネットのセキュリティはこの数十年で劇的に改善しましたが、最新技術の全般的な健全性にはいくつかの重大なギャップが見られます。そのギャップが最も顕著なのは、IoT 技術における 2 つの主要コンポーネントである、埋め込みシステムとクラウドサービスです。

多数のユーザーグループと物理的システムを危険にさらすことなく IoT を発展させるためには、エンドポイントと IoT サービスの両方で情報セキュリティ対策を徹底する必要があります。

- プロジェクト開始時点において、セキュリティのベストプラクティスが製品やサービスに組み込まれているか。
- ソフトウェアや製品の開発ライフサイクルの中に、セキュリティのライフサイクルが組み込まれているか。
- アプリケーションのセキュリティは、埋め込みシステム上で作動するサービスとアプリケーションの両方に適用されているか。
- トラステッド・コンピューティング・ベース（TCB）は、エンドポイントとサービスのエコシステムの両方に実装されているか。
- TCB による、アプリケーションの画像とサービスの自己確認はどのように実行されるか。

- 構成やアプリケーションに異常があった場合、エンドポイントや IoT サービスは検出できるか。
- 悪質行為を示唆する異常に対して、エンドポイントをどのようにモニターするか。
- 認証および ID は、製品やサービスのセキュリティプロセスとどのように関連するか。
- セキュリティ侵害を示唆する異常の検出に対して、インシデント対処計画をどのように定めているか。
- セキュリティ侵害を迅速かつ効果的に阻止できるようにするために、サービスとリソースをどのようにセグメント化するか。
- セキュリティ侵害が生じた後、サービスとリソースをいかにして復旧するか。
- 攻撃を検出できるか。
- セキュリティ侵害を受けたシステムコンポーネントを検出できるか。
- 顧客はどのようにしてセキュリティに関する懸念を報告できるか。
- 脆弱性を排除するために、エンドポイントをアップデートしたり、パッチを提供したりできるか。

# 3 モバイルのソリューション

IoT の接続性を解決する技術は無数にあるものの、IoT の未来を築くにあたってモバイルネットワークほど優れたものはありません。モバイルネットワークは 20 年以上前に、消費者と産業を対象とした初のワイヤレスサービスを提供し、その後も常に、信頼性と可用性の高い、安全かつ費用対効果に優れたサービスを提供してきました。長距離にわたって運用する無線通信ネットワークが不安定な性質だったことから、モバイル業界はネットワークの可用性に関して豊富な経験を有しています。ネットワーク識別が課題とされてきたことから、そこから数々の仕様、デバイス技術、プロトコル、分析モデルが誕生しました。プライバシーとセキュリティはモバイル業界が絶えず懸念する問題であり、あらゆるモバイル技術で悪用や ID の乗っ取り、不正が生じる可能性を減らす取り組みが行われてきました。

モバイル業界は、IoT アプリケーションとサービスのニーズに対応するために、規格に準拠したライセンス取得済みのローパワー・ワイドエリア（LPWA）ワイヤレスネットワーク技術（NB-IoT および LTE-M）を提供しています。このような LPWA ネットワーク技術は、円滑な通信に必要なわずかな電力を用いて、従来のモバイルネットワークと同程度の対応エリア（多くの場合はエリアが拡大しています）とワイヤレス接続を実現します。ネットワーク事業者の多くは LPWA サービスを展開しているため、NB-IoT と LTE-M が LPWA ネットワークの展開の実質的な基準となることでしょう。

世界各地の NB-IoT および LTE-M ネットワークの展開に関する詳細については、GSMA 公式ウェブサイト（https://www.gsma.com/iot/mobile-iot-initiative/）を参照してください。

## 3.1 可用性の課題への対処

GSMA の「モバイルエコノミー2017」報告書[1]に、以下の説明があります。

- モバイル業界は引き続き急速に拡大しており、2016 年末の時点でユニークモバイル加入者は計 48 億人に達している。2020 年までにユニークモバイル加入者は世界の人口のおよそ 4 分の 3（57 億人）に達すると予想されている。
- モバイルのブロードバンドネットワークへの技術シフトの動きが引き続き世界中で加速している。モバイルのブロードバンド接続（3G と 4G の技術）は、2016 年末の時点では総接続数の 55%に満たなかったが、2020 年までにおよそ 4 分の 3 に増加するとみられる。4G 接続の割合は、今後 10 年間で 23%から 41%に増加し、およそ 2 倍となると予想される。
- 2016 年から 2020 年の間にモバイルのブロードバンド接続数が 23 億増加するとみられており、全体の 73%を占めると予想される。2016 年には 4G 接続数が 17 億まで増加し、全体の 55%を占めたことから、4G への急速な移行は例年に続いて 2016 年の大きな特徴となっている。その結果、2020 年までに 2G は主要な接続技術ではなくなると予想される。
- LPWA デバイスに対応できる世界市場は大きな規模を誇っており、2020 年までに同デバイスへの総接続数はおよそ 14 億まで増加するとみられる。一部の業界研究者は、2022 年までにその数は 50 億まで拡大すると予想している。

## 3.2 ID に関する課題への対処

ID の管理は数十年前から課題とされてきましたが、モバイル業界の標準や技術提供はこの課題のおかげで大いに強化されてきました。モバイル業界では一般に取り外し可能な SIM カードを連想しますが、GSMA は「埋め込み SIM のリモート・プロビジョニング・アーキテクチャ」[2]という SIM をベースとするソリューションを開発しました。これは IoT での利用に適したソリューションであり、下位のコンポーネントレベルでのエンドポイントデバイスへの組み込みや、製造コストの削減、全耐用期間における IoT エンドポイントデバイス接続の有効化、OTA（Over-The-Air）プラットフォーム経由の接続管理が可能になります。

埋め込み SIM をはじめとする識別技術は、デフォルト設定でセキュリティを組み込んだトラストアンカーとして設計されています。このような識別技術は、次のような攻撃を阻止するためのものです。

- 異常発生
- サイドチャネル分析
- 受動的データ傍受
- 物理的改ざん
- ID の乗っ取り

既にセキュリティがこのように強化された技術に対して、さらに卓越した進化を実現することは、これら新世代のトラストアンカーによって、IoT を巡る状況に重要な変化がもたらされることを意味します。これらの技術には二重の用途があり、ネットワークのセキュリティ検証だけでなく、従来型のコンピューターのトラストアンカーと同様、アプリケーション通信とアプリケーション自体のセキュリティ保護にも利用できるようになります。

3GPP GBA [8]、OMA [11]、oneM2M [12]をはじめとするモバイル業界のセキュリティ仕様を統一することによって、この二重用途の機能は更に拡張するでしょう。これらの技術は、デバイスをフィールドに安全に設定し、OTA によるファームウェアのアップデートを可能にし、デバイスの機能と ID を管理するのに役立ちます。

これらの技術を併用することで、現在の複雑なエンジニアリング・プロセスが容易になり、1 つの単純なコンポーネントに統合されます。アプリケーション・エンジニアが自分で管理する必要がある複雑な技術を構築するのではなく、ネットワークの ID を管理しているネットワーク事業者がアプリケーションの代行としてこれを実施することができます。それによって、エンジニアリングの複雑性を低減するだけでなく、事業の日常管理での必要事項も減少します。

## 3.3 プライバシーとセキュリティに関する課題への対処

モバイル業界は SIM 機能と同時にセキュリティを確保し、不正やその他の悪質行為の可能性を軽減するために、強固なプロトコルやプロセス、モニタリングシステムを開発してきました。例えば、3G および 4G の技術では、エンドポイントとネットワークの ID の確認に相互認証が用いられています。このプロセスは、攻撃者による通信の傍受を阻止するのに役立ちます。

また、ネットワーク技術は、GBA [8]や EAP－SIM [9]などの技術と SIM を利用してセキュリティを保護することもできます。これらの技術を用いることで、よく知られたプロトコルに従ったアプリケーションネットワーク内のピアとの通信に使用できるセッション・セキュリティキーを、SIM に搭載できます。このプロセスによって、攻撃者がアプリケーションプロトコルを操作してデバイスやサービスのセキュリティを侵害するリスクを低減できます。このように、このモデルではネットワークとアプリケーションの両方の安全を確保することが可能となります。

# 4 IoT モデル

以下の図は、一連の文書全体で使用する標準的な IoT モデルを、サービスのエコシステムとエンドポイントのエコシステムのコンポーネントとして示したものです。各コンポーネントはサブコンポーネントから構成され、文書ではその主な要素だけを取り上げて説明しています。例えば、本文書群において、エンドポイントとその各リスクは「エンドポイントのエコシステム」文書[3]に、サービスは「サービスのエコシステム」文書[4]に概説されています。


**図 2 - IoT モデルの例**

上の図を見ると、現在のほぼすべての IoT サービスや製品モデルについて、生産準備が整った（production-ready）技術を実装するにあたって必要となる主なコンポーネントがわかります。

通信回線は IoT 固有のコンポーネントであり、このモデルにおいては、通信リンクのそれぞれの「末端」がある 2 つのエコシステム（該当する「エンドポイントのエコシステム」文書と「サービスのエコシステム」文書に説明があります）の間の接続を提供するものです。

ネットワーク事業者向けのネットワークのセキュリティ・ガイドラインに関する推奨事項については、GSMA の「ネットワーク事業者向けの IoT セキュリティ・ガイドライン」[13]を参照してください。

## 4.1 サービスのエコシステム

サービスのエコシステムとは、フィールドで展開するエンドポイントに機能を提供し、そこからデータを収集するために必要な一連のサービス、プラットフォーム、プロトコルおよびその他の技術を指します。サービスのエコシステムは、通常エンドポイントからデータを収

集し、サーバー環境にデータを保存します。このデータを簡潔な視覚表示として各種ユーザーインターフェイスに送信することにより、データをユーザーに提示することができます。多くの場合、データはメトリクスやパラメーター、コマンドの形式で、サービスインフラ由来の API（oneM2M [12]）を経由して認証を受けた第三者に受け渡すこともでき、IoT サービス提供者がサービスを収益化するための一般的な方法となっています。

本概要説明書に記載されているプロセスとの関連で参照すべきサービスのエコシステムに関するセキュリティ・ガイドラインについては、CLP.12「IoT サービスのエコシステムに関する IoT セキュリティ・ガイドライン」[4]を参照してください。

### 4.2 エンドポイントのエコシステム

エンドポイントのエコシステム[4]は、複数の種類の有線・無線ネットワーク経由で現実の世界とデジタルの世界を接続する、複雑性の低いデバイス、リッチデバイス、ゲートウェイから構成されます。一般的なエンドポイントの例には、警報装置、デジタル・ドアロック、自動車用のテレマティクスシステム、センサー駆動型の産業用制御システムなどがあります。エンドポイントは周囲の物理的環境からデータを収集し、キャピラリーネットワークやセルラーネットワークを経由して、それを各種フォーマットでサービスのエコシステムに配信します。大抵はその応答として指示やアクションを受けます。エンドポイントまたはサービスのエコシステムから取得したデータを表示する、リッチ・ユーザー・インターフェイスがエンドポイントに含まれる場合もあります。

本概要説明書に記載されているプロセスとの関連で参照すべきエンドポイントのエコシステムに関するセキュリティ・ガイドラインについては、CLP.13「IoT エンドポイントのエコシステムに関する IoT セキュリティ・ガイドライン」[13]を参照してください。

## 5 リスク評価

リスク評価の概念は何十年も前からあるものですが、多くの企業にとって、情報セキュリティよりも全般的なビジネスリスクの方が評価対象として浸透しています。しかし、事業の技術面における安全性の高い運用や長期継続には、情報セキュリティのリスク評価プロセスも欠かせません。エンジニアチームが事業の成否のカギを握る「モノのインターネット」の技術において、リスク評価プロセスが組織のセキュリティ対策の第一歩となることは明らかです。

あらゆる組織に対して技術リスクを詳細に把握する視点が求められる一方で、次のような専門性の高い問いが情報セキュリティのリスク評価プロセスの出発点となります

- 保全が必要な資産（デジタル資産または実物資産）はどれか。
- 潜在的な脅威アクターに該当する集団（実体のあるものまたは実体のないもの）は何か。
- 組織にとって脅威となるものは何か。
- 脆弱性は何か。
- 保全資産のセキュリティが侵害された場合、どのような影響があるか。
- 保全資産のセキュリティが侵害される可能性はどの程度か。

- 別の攻撃者*グループ*の存在も考慮すると、どのような影響があるか。
- 組織およびパートナーにとって、資産の価値はどれくらいか。
- 資産のセキュリティが侵害された場合、安全面でどのような影響があるか。
- 潜在的な脆弱性を是正または緩和するために何ができるか。
- セキュリティの新たなギャップや拡大するギャップをどのように監視できるか。
- 解決できないリスクは何か、またそれは組織にとって何を意味するか。
- インシデント対策、モニタリング、リスク是正のための予算はどうするか。

以上の点が、組織においてエンジニア・IT チームが有効に機能するための出発点となります。目指すべきゴールは、事業の技術面を、経営面におけるリスク、価値、是正計画と確実に一致させることです。チームの連携を推進することによって、事業リスクだけでなく資産価値も考慮した、より現実に即した視点が得られます。これは、未対応のセキュリティギャップに充てるべき予算に直接影響を及ぼすでしょう。

リスクによっては絶対に解消できないものがあります。本ガイドラインではその一部を取り上げます。組織はこれらのリスクを評価し、許容できるものであるかどうかを判断しなくてはなりません。これにより、事業の限界や技術上の制約、特定の脅威への対処を現実に即して理解することができます。費用対効果が高い方法ですべてのセキュリティギャップを解消できるという発想では、予算がいくらあっても足りません。

## 5.1 目標

リスク評価の目標は、組織のテクニカル部門において見られるセキュリティギャップを是正、監視および対応するための一連のポリシーや手順、管理体制を策定（またはアップデート）することです。リスク評価の結果は、企業が技術面そのものだけでなく、技術を管理・設計・配備する方法を修正する手助けとなります。リスク評価の結果により、組織内で使用されている情報とリソースの価値がより明らかになり、人事、作業プロセス、ポリシーの改善を通じて、企業全体のさらなる強靭化を図ることができます。

リスク評価の結果を利用することには、以下のような利点があります。

- 従業員への告知
- プロセスの改善
- ポリシーの設定（またはアップデート）
- 是正策の実行
- 新たなギャップの監視
- 製品またはサービスの向上

これらの利点は、組織の人事とプロセス上のセキュリティの基本プラットフォームを本質的に強化することになります。このプラットフォームを、組織全体の役割と責任を継続的に評価・改善していくサイクルに組み込む必要があります。

## 5.2 リスクモデル参照

ここでは、リスク評価や脅威モデルのプロセスについて詳細な説明を省略します。以下の参考資料にリスク評価のプロセスについて適切な説明と解説がなされていますので、内容をご確認ください。

- アメリカ国立標準技術研究所（NIST)の「リスク管理フレームワーク」[5]
- コンピューター緊急対応チーム(CERT)の OCTAVE モデル[6]

# 6 プライバシーの検証

多くの IoT の製品やサービスは、データの作成、収集または共有を目的として設計されます。これらのデータの一部は「個人データ」とはみなされず、消費者のプライバシーには影響を与えないため、データ保護やプライバシーに関する法律の対象とはなりません。例えば、マシンの物理的な状態や内部の分析データ、またはネットワークの状態を表すメトリクスなどがそれに該当します。

しかし、多くの IoT サービスには、個人の消費者に関するデータが含まれており、一般的なデータ保護とプライバシー関連法律の適用対象となっています。モバイル事業者が IoT サービスを提供する場合、通信業界特有のプライバシーとセキュリティに関する規制の対象となります。「消費者」向けの IoT サービスは、詳細な個人データの作成・配布・使用を伴うため、個人のプライバシーに影響を与える可能性があります。例えば、個人の健康状態を推測するものや、買い物の傾向と場所から個人のプロファイルを導き出すものなどが挙げられます。消費者 IoT サービスの人気が高まるにつれて、リアルタイムでより多くの消費者データが作成・分析され、国境をまたいでそれらが数多くの当事者の間で共有されることになるでしょう。

データが特定の個人に関連する場合、この複雑に「結びついた」エコシステムについて、消費者は以下のような疑問を持つかもしれません。

- 個人データを収集、共有および使用しているのは誰か。
- 具体的にどのようなデータが収集されているのか。
- どこから（どのような技術またはインターフェイスで）データが取得されているのか。
- いつデータが収集されているのか。
- なぜユーザーからデータが収集されているのか。
- 個人情報の(安全性だけではなく)プライバシーはどのように確保されるのか。
- データの共有手段や企業の使用方法に関して、個人がコントロールできるのか。

個人データに依存するすべての IoT サービス提供業者や、そのデータを取得または利用するパートナー企業は、個人のプライバシーを尊重し、個人を特定したりプライバシーを侵害したりするような情報を安全に管理する義務があります。

IoT のサービス提供者にとって重要な課題となるのは、プライバシーとデータ保護に関する複数の法律があり、多くの場合これらの法律に矛盾が見られることです。関連するデータによって、またサービス提供者が提供するサービスや業界によって、異なる国で異なる法律が適用されるかもしれません。これは多くの消費者向け IoT サービス提供者に関係することです。

例えば、コネクテッドカーが国境をまたいで移動すると、複数の異なる司法権の下で関連するデータがやり取りされることになります。車両搭載のセンサーで車の位置を（静的または動的に）把握し、頻繁に行く目的地を追跡すれば、運転手のライフスタイルや趣味、宗教な

ど、運転手が個人情報と考える多くの特性が導き出され、それらが使用されるかもしれません。さらに「車載の診断」センサーにより、運転傾向から導き出せる情報が保険会社と共有され、保険会社はそれを利用して高い保険料を請求することも考えられることから、運転手自身が知らないうちに差別を受ける可能性もあります。

他の IoT のサービスやデバイス（コネクテッドカーを含む）も、異なる国家領域を移動し、異なった法体系の間を移動することができます。多くの場合、居住国以外の法律に従って個人データが移動または保管されます。これらの問題は、今後多国籍 IoT サービスが展開されるまでに検討されるべき重要な問題です。

もう 1 つの課題は、ある種類の「個人データ」（健康に関するデータなど）を利用する前に、影響を受ける消費者（「データ主体」ともいう）の同意を得ることを、多くのデータ保護の法律が消費者データを収集する企業に要求していることです。多くの法律では、「個人データ」を、特定の個人として「識別された」または「識別することができる」生きた自然人に関する全ての情報と定義しています。

しかし、法律上で「個人の」ものと解釈されない情報でも、インターネットに接続されるデバイスが増加すると、個人に関するより多くのデータが収集・分析され、個人のプライバシーに影響を与える可能性があります。大量のデータとクラウドストレージに予測分析を組み合わせることで、ユーザーの詳しいプロファイルを提供できます。個人情報はその他のデータタイプから導き出すこともでき、完全な匿名情報のままにしておくことは極めて困難となる恐れがあります。

健康データなど、取り扱いに配慮が必要な記録のプライバシーを維持する必要性は、そのような記録が業務上で悪用される可能性もあることから、特に強く認識されています。米国では、医療保険の相互運用性と説明責任に関する法令（HIPAA、1996 年）に、健康上の記録の不正開示に関するリスクを緩和するために、プライバシーと安全性の要件が盛り込まれています。

欧州連合の他の多くの規制と同様に、HIPAA も健康上のデータが *特定の個人として識別され得る* 場合にのみに適用されます。血液モニターデバイスに蓄積されたデータは（ユーザーを特定しないため）このような要件の対象外となりますが、スマートフォンのアプリやクラウドサーバーのデータは、（スマートフォンにはほぼ確実に個人を特定するその他のデータが含まれており、クラウドサーバーはユーザーを特定できるアカウントに紐付けられており）個人の特定が可能なため、規制の対象となるでしょう。世界中の政策担当者は、「特定の個人として識別され得る」と定義されていなくても、人々に関する情報や知見がプライバシーに影響を与える可能性があることを認識しています。そのため、政策担当者はリスクに基づいた規制アプローチを重視し始めており、法律上の定義に注意を向けるのではなく、データの利用がプライバシーに幅広く影響を与えることを考慮し始めています。

IoT のエコシステムの信頼性を構築するために、各国の政府はデータ保護とプライバシーに関する法律が技術に影響を与えず、インターネットエコシステムの全ての参加者に一貫したルールが適用されること保証する必要があります。また、IoT サービス提供者は、規制による不必要な介入を避けるため、IoT サービスや製品の開発初期段階で、付属文書 A に記載されている手順に従うことが推奨されます。

# 7 本ガイドラインの有効な使い方

セキュリティはエンジニアリングプロジェクト開始時に実装することが最も効果的ですが、本ガイドラインは、IoT サービスや製品を設計済みまたは組立終了済み、さらには既に展開している組織にも役立ちます。読者の製品またはサービスがどの段階にあるかに関わらず、本ガイドラインを最大限活用するために以下の手順に従う必要があります。

- テクニカルモデルの評価
- 現在のサービスまたは製品のセキュリティモデルの見直し
- 推奨事項の見直しと評価
- 実装と見直し
- ライフサイクルの継続

## 7.1 テクニカルモデルの評価

最も大切な最初のステップは、組織の IoT サービスまたは製品への理解を深めることです。セキュリティの見直しとリスク評価を行うにあたり、担当チームは組織のソリューションで使用されている各コンポーネントを熟知する必要があり、コンポーネント間の関係と、コンポーネントと環境との関係を理解する必要があります。製品またはサービスがどのように作られているのか（またはこれから作られるのか）をしっかりと理解しなければ、見直しは不十分なものになるでしょう。

まず、システムで使用されているコンポーネントを説明する文書を作成しましょう。各コンポーネントのソース、使用方法、必要な権限レベル、ソリューション全体への統合方法を確認します。エンドポイントエコシステム[3]とサービスエコシステム[4]のガイドライン文書にあるモデルセクションに記載されている技術に、各コンポーネントをマッピングします。文書は一般的なクラスにマップすれば良いので、特定のコンポーネントに合致しなくても問題ありません。マイクロコントローラーやコミュニケーションモジュール、トラストアンカーなど、前後関係に沿ってコンポーネントのクラスを使用してください。以下のような質問に対する答えを考えてみましょう。

- 製品またはサービスを作るために、どのようなコンポーネントが使用されているか。
- 特定のコンポーネントに対して、どのようなインプットとアウトプットが適用できるのか。
- 該当するインプットとアウトプットに既に適用されているセキュリティ規制は何か。
- コンポーネントに適用される権限レベルは何か。
- 組織内でコンポーネントを実装する責任者は誰か。
- 組織内でコンポーネントを監視および管理する責任者は誰か。
- コンポーネントで検出されたリスクを是正する手順は何か。

これらの質問に答えることにより、技術的なコンポーネントがお互いにどのように関わり合っているのか、製品またはサービス全体が各コンポーネントからどのような影響を受けるのかを理解することができます。

このプロセスは、CERT/OCTAVE のリスク評価モデル[6]の第 1 および第 2 フェーズ、または NIST のリスク管理フレームワーク[5]の「フレーム」段階にあたります。このテクニカル

モデルの評価は、重要なビジネス資産のプロファイルの開発や安全性に関する目標の確立に役立つとともに、企業がリスクの評価、監視および対処するための基盤を構築します。

## 7.2 現在のセキュリティモデルの見直し

次に、評価対象となるエンドポイントまたはサービスの「セキュリティモデル」セクションを参照してください。同セクションを参照することで、攻撃者が特定の技術に対するセキュリティ侵害を引き起こすために利用するモデルについて理解を深めることができます。このモデルは、リバースエンジニアリングや埋め込みシステムのセキュリティ評価を実施した長年の経験に基づいています。

セキュリティモデルの見直しを完了することで、開発中の製品またはサービスにとってどの技術が最も価値があり、攻撃者対策に望ましいのかについて理解が深まっているはずです。見直しによって得られた情報を組織内で共有し、エンジニアとチームリーダーがともに現在のモデルに対するリスクと脅威を確実に理解する必要があります。

しかしこの時点では、組織としてはまだセキュリティモデルの修正をする段階では*ない*ということに注意してください。この時点で大まかなアーキテクチャ変更をするのは時期尚早です。

このプロセスも、CERT/OCTAVE のリスク評価モデル[6]の第 1 および第 2 フェーズ、または NIST のリスク管理フレームワーク[5]の「フレーム」段階にあたります。セキュリティモデルの見直しは、潜在的な安全性のギャップを特定することで、優先すべき安全性に関する目標に焦点を当てることができ、テクニカルモデルの強化に役立ちます。

## 7.3 推奨事項の見直しと評価

セキュリティタスクを解決するための考えられる方法を評価するために、この段階で*推奨事項*のセクションを見直すべきでしょう。このセクションでは、単に推奨事項を実装する方法が示されているだけでなく、特定の推奨事項を実装するにあたっての課題に関する知見も示されています。

各推奨事項に対して*方法*のセクションが設けられています。このセクションには、対象となるセキュリティリスクの是正または緩和をサポートする方法の概要が記載されています。これらの方法は専門的な見地に基づいて解説されていますが、合理的かつ現実的な努力レベルで最大限の改善が得られるよう、リスクを包括的な視点から軽減するためのコンセプトの概要が示されています。

また*費用*セクションでは、特定の推奨事項を実装する場合に、組織として準備すべき追加予算（必要な場合）について解説しています。エンジニアリング時間や原材料など、ほとんどの費用は明確化することができますが、既に企業の経営陣によって予算や利益率が決まっている製品またはサービスに対して必要予算を変更する結果となるような、確定できない費用も示される可能性があります。特定の費用の金額は示されませんが、追加費用が発生する可能性がある技術やサービスが提示されます。

特定の推奨事項を実装しなかった場合のセキュリティギャップを読者が理解できるように、*リスク*セクションも設けられています。ビジネス上ある程度のリスクは運用上のガイドラインの範囲内として許容されるかもしれませんが、読者はそれぞれの「リスク」セクションを見直し、特定の推奨事項を実装しなかった（または適切に実装しなかった）場合の副次的影響を、自社が完全に理解しているかどうかを確認する必要があります。例えば、「データの暗号化」のような推奨事項は明確で分かりやすいですが、暗号上一意的でないメッセージに対する再生攻撃のような巧妙な脅威は、後に想定外の事態を引き起こす恐れがあります。

また、詳細な見直しを行うための*参考文献*が示される場合もあります。本文書には全ての技術やリスク、是正計画についての詳細な情報は記載されていませんが、他の基準や実証済みの戦略には提示されています。本文書では、各推奨事項において、必要に応じて該当する基準や戦略に関する参考資料を提示しています。

「推奨事項」セクションの見直しの結果は、「セキュリティタスク」セクションに直結します。この段階では、セキュリティタスクを適切に実装するために、セキュリティタスクに適切な推奨事項が盛り込まれているはずです。次に、これらのセキュリティタスクを組織の担当者に割り当てられている特定のコンポーネントに関連付けられます。

推奨事項の評価は、NIST リスク管理フレームワーク[5]の「評価」段階、CERT/OCTAVE の方法論[6]のステップ 6、7、8 に該当します。

## 7.4 実装と見直し

この段階では、セキュリティタスクの概要が明確になっており、企業はセキュリティ上の脆弱性、価値およびリスクについてより深い理解を得ているはずです。企業は修正が必要な各コンポーネントに対する明確なアーキテクチャモデルを作成します。そして、各コンポーネントとセキュリティタスクに適した推奨事項とリスクを考慮しながら、企業が採用したリスク評価プロセスを使用して、各コンポーネントの脅威モデルを開発します。アーキテクチャモデルが完成すると、セキュリティタスクを遂行するために各推奨事項の実装に取り掛かることができます。

実装が完了すると、企業は「推奨事項」のサブセクションと「コンポーネント」セクションにおいてリスクを見直す必要があります。企業は、これらのセクションで設定された要件を実装後に満たしていることを確認しなければなりません。これらの文書は業界で設計された全ての製品またはサービスを完全に網羅することはできないため、企業は、自社の製品またはサービスにおいてコンポーネントが設計されたコンテキストに添って、実装がセキュリティの問題を解決していることを確認する必要があります。可能であれば、第三者のコンサルティング会社に、セキュリティに関するベストプラクティスが実装されているかどうかについて評価を行うことを依頼してください。

実装と見直しは、NIST リスク管理フレームワーク[5]の「対応」項目、CERT/OCTAVE モデル[6]のステップ 8 に該当します。

### 7.5 ライフサイクルの継続

この段階で、セキュリティのライフサイクルが終了するわけではありません。セキュリティはプロセス全体のエンジニアリングの不可欠な部分となっています。エンドポイントと IoT サービスには寿命があり、その寿命が続く限り、生き物と同じように世話をしなければなりません。

要求事項は時とともに変わっていきます。暗号化アルゴリズムは、陳腐化したり廃止されたりします。そのような変化に対応するために、製品またはサービスで新たなプロトコルや無線技術を相互運用する必要があります。埋め込み型の製品が装備され、絶えず変化するこのエコシステムは、匿秘性、正当性、可用性、信頼性が確実に維持されるよう、常に見直しが必要となります。

継続的なセキュリティライフサイクルの管理は、NIST リスク管理フレームワーク[5]の「監視」と「フレーム」項目、CERT/OCTAVE モデル[6]のステップ 1、4、5 が該当します。

## 8 事例 - ウェアラブル心拍数モニター

この事例では、本ガイドラインを使用してシンプルな心拍数モニター（HRM）の設計の評価を行います。エンドポイントの評価はエンドポイントエコシステムの文書を使用し、サービスはサービスエコシステムの文書を使用して評価します。

### 8.1 エンドポイントの概要

まず、エンドポイントのハードウェア設計の評価から始めましょう。

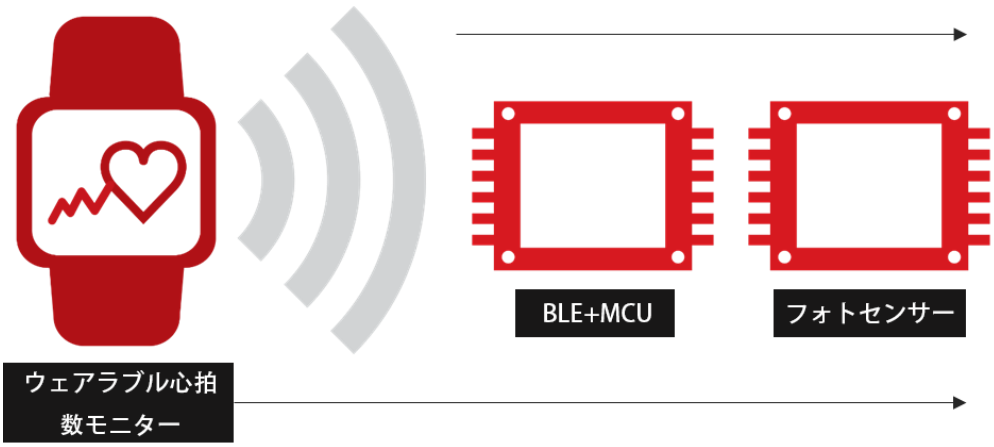


**図 3- シンプルな心拍数モニター（HRM）と主なコンポーネント**

HRM は、環境照明フォトセンサーと、Bluetooth 低エネルギー（BLE）トランシーバーで稼働するマイクロコントローラーというシンプルなワイヤレスのウェアラブルデバイスの標準的なコンポーネントから成り立っています。センサーは脈拍データ採取に使用され、マイクロコントローラーはセンサーから送られてくるデータを分析し、内蔵された BLE トランシーバーを介してどのデータを送るかを選別します。この事例で使用されている BLE スタックはバージョン 4.2 です。

HRM からスマートフォンやタブレットなどの他のデバイスにデータを転送するために、この事例ではコイン電池バッテリーが使用されています。このデバイスを作動させるために、その他のコンポーネントは必要ありません。

エンドポイントエコシステムの文書によれば、このデバイスは軽量エンドポイントクラスに分類されるでしょう。

## 8.2 サービスの概要

サービスについては、スマートフォンやタブレット上のアプリケーションが、エンドポイントから利用可能なネットワーク接続を通してバックエンドサービスまでメトリクスを送信します。アプリのバックエンドサービスは、単純に収集されたメトリクスとデバイスの所有者を関連付けて、アプリのサーバーのローカルなデータベースに保存するだけです。

データの視覚化はモバイルのアプリか、またはそのサービスのウェブサイトで行うことができます。ウェアラブルテクノロジーのユーザーはサービスプロバイダのウェブサイトにログインし、エンドポイントで収集されたメトリクスを利用してさらに多くの操作を行うこともできます。

これはカスタム性がなく、過剰な複雑性もない非常にシンプルかつ一般的なサービスモデルです。

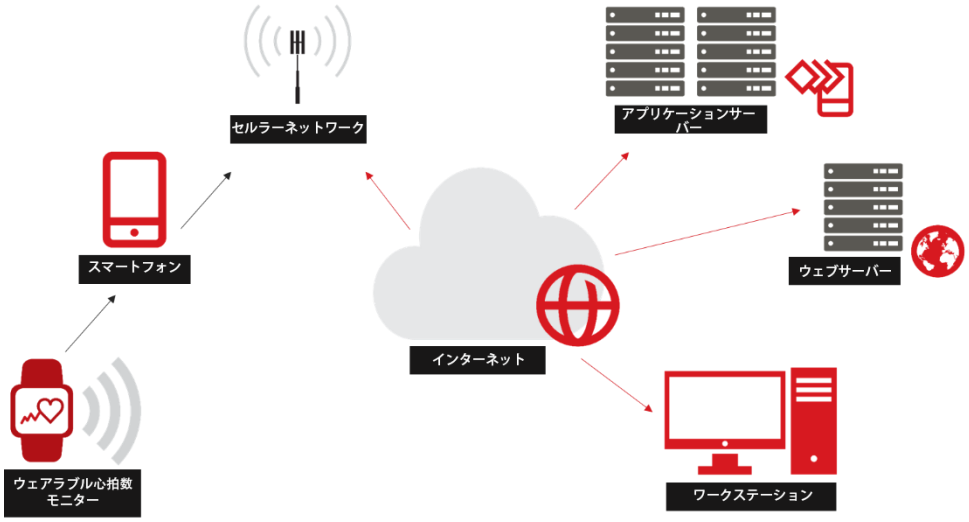


**図 4- シンプルなバックエンドサービスへのデータフロー**

## 8.3 使用例

この技術を開発する企業は、エンドユーザーが 1 日を通して心拍数データを収集し、データをアプリとバックエンドのデータベースに保存することを想定しています。つまり、ユーザーが自分の心拍数を長期間にわたって確認し、総合的な健康管理を行うことを意図しています。ユーザーは、健康なライフスタイルを維持しているかどうかによって、自分の健康が改

善または悪化しているのを確認することが可能です。これにより、ユーザーは自分の HRM のデータの改善傾向や悪化傾向を確かめながら、目標達成の意欲を高めることができます。

この場合、企業は、医療装置メーカーや医療サービスの提供者、心臓発作や脳卒中などの健康に関連した症状を起こしやすいユーザーを特定するためのメトリクスを使用できるその他のパートナーとともに、このデータを利用しようと考えています。

## 8.4 セキュリティモデル

この事例の企業のエンジニアリングチームは、自社の製品またはサービスに最も関係がある問題を特定するために、エンドポイントとサービスの文書の「セキュリティに関するよくある質問」セクションを活用しました。

その結果、エンドポイントの観点からは、以下のような問題点があることがわかりました。

- クローニング
- エンドポイントのなりすまし
- サービス上のなりすまし
- プライバシーの確保

一方、サービスの観点からは、以下の問題点を特定しました。

- クローニング
- サービスのハッキング
- エンドポイントでの異常な動作の特定
- セキュリティ侵害の制限
- データロスの削減
- 搾取の削減
- ユーザーのプライバシーの管理
- 可用性の向上

チームは、関連する「セキュリティに関するよくある質問」セクションに従って、上記のそれぞれの問題に対する推奨事項を見直し、費用対効果が高く、最大のセキュリティを確保できる改善案の推奨事項を実装することにしました。

この事例のモデルでは、エンドポイントでの大きな変更は必要ないでしょう。エンドポイントでの機能は限られているため、エンドポイントではアプリの安全性と通信の両方に対して最低限のセキュリティを備えるだけで済みます。エンドポイントのアプリは単一のデバイスで稼働しているため、デバイスのファームウェアが *ロックされている*限り、この事例の使用方法では実際に攻撃を受ける恐れはありません。

しかし、プライバシーの問題が残っているため、企業は少なくともトラステッド・コンピューティング・ベース（TCB）の個人向け PSK バージョンを使用する必要があります。これにより、暗号トークンは各エンドポイント固有のものとなり、1 つのエンドポイントがセキュリティ侵害を受けたことにより、その被害が全てのエンドポイントに及ぶことを防ぐことができます。個人用の（固有の）鍵がロックされたマイクロコントローラーにエンコードさ

れている場合、この使用例はクローニングやなりすまし、プライバシー問題の脅威から十分に保護されていると言えるでしょう。各エコシステム内で使用されているトラステッド・コンピューティング・ベース（TCB）に関する詳細については、IoT サービスの文書[3]とエンドポイントの文書[4]を参照してください。

一方、サーバーのインフラストラクチャには大きな変更が必要です。推奨事項に従って見直しを行った結果、エンジニアたちは重大な悪用リスクがあることに気付き、次のような問題を確認しました。

- サービス拒否攻撃の影響を抑えるフロントエンドのセキュリティがない。
- サービスからの、またはサービスへのトラフィックのフローを制限する、入口・出口のコントロールがない。
- サービス部門間で職務の分離が行われていない。
- 個人向け PSK トークンを含む、分割された安全データベースがない。
- サービスオペレーティングシステムで、適切なセキュリティ措置が実施されていない。
- エンドポイントでの異常な動作を評価するメトリクスがない。

## 8.5 結果

ガイドラインによって特定されたリスクに対して適切に対処できるように推奨事項を実装したことで、企業のバックエンドサービスのアーキテクチャは大幅に改善されました。

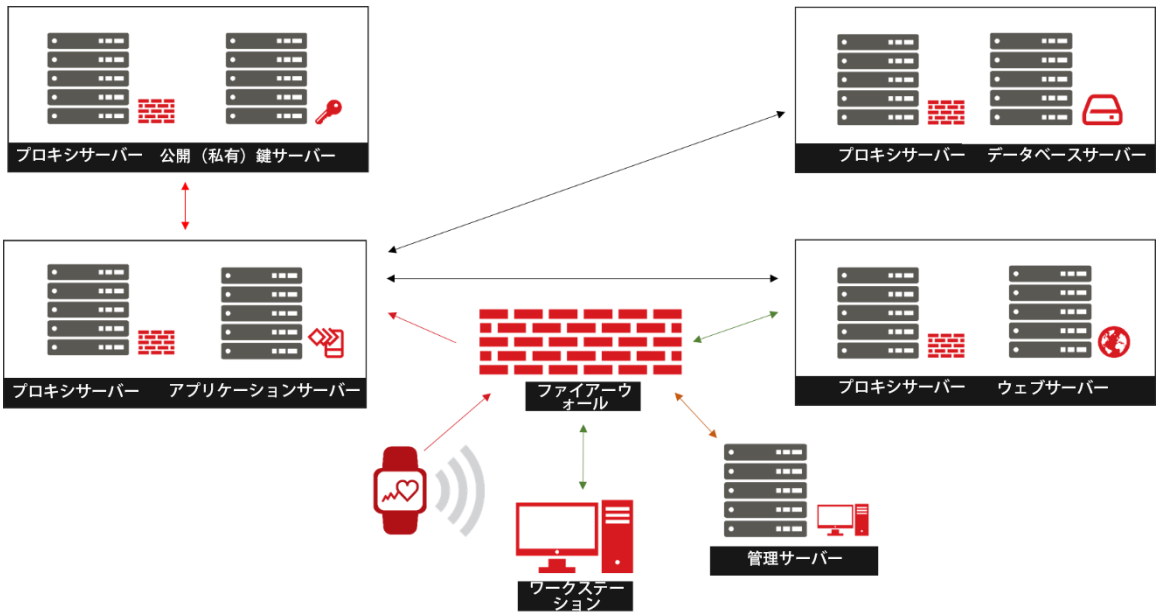


**図 5- 改善後のサービスエコシステム**

上の図でサービスエコシステムの変化は一目瞭然です。安全性を高めるため、各サービスクラスは別々の階層に分けられ、需要が急増した場合には、その技術を容易に拡張することができます。外部の世界と直接相互作用するサービスと重要なシステムを分離するために、デ

ータベース層と認証層の 2 つの層が追加されました。システム全体の可用性を低下させる DoS や DDos 攻撃など、さまざまな種類の攻撃から内部ネットワークを保護するために、セキュリティフロントエンドが実装されました。最後に、本番環境への管理者のアクセスを確保するために、管理モデルが定義されました。上記の図に示されていないコンポーネントに分析モデルがありますが、これはエンドポイントの動作がセキュリティ侵害を示すタイミングや、ファームウェアまたはハードウェア設計上の欠陥を監視するものです。

### 8.6 要約

総合的に見て、もし現状のままで使用されていれば、このシンプルな技術は簡単にセキュリティ侵害を受けていたでしょう。しかし、エンドポイントでシンプルかつ費用対効果の高い複数の変更を迅速に実施すれば、この技術はアーキテクチャを変更することなく同じ分野で長期にわたって有効となるでしょう。

サービスエコシステムの拡大に伴い、ユーザーと企業に対する脅威はどんどん少なくなっていきます。クローニングとなりすましはもはや脅威ではありません。各エンドポイントに固有の暗号トークンを付与することで、プライバシーは保護されます。重要な情報を格納しているシステムは、頻繁に悪用される一般向けシステムからは隔離および保護されています。モデルは多少複雑にはなったものの、本番環境全体のリスクは軽減されています。

## 9 事例 - 個人用ドローン

この事例では、本ガイドラインを使用して小型の個人用ドローンの評価を行います。エンドポイントの評価はエンドポイントエコシステムの文書を使用し、サービスはサービスエコシステムの文書を使用して評価します。

### 9.1 エンドポイントの概要

まず、エンドポイントのハードウェア設計の評価から始めましょう。

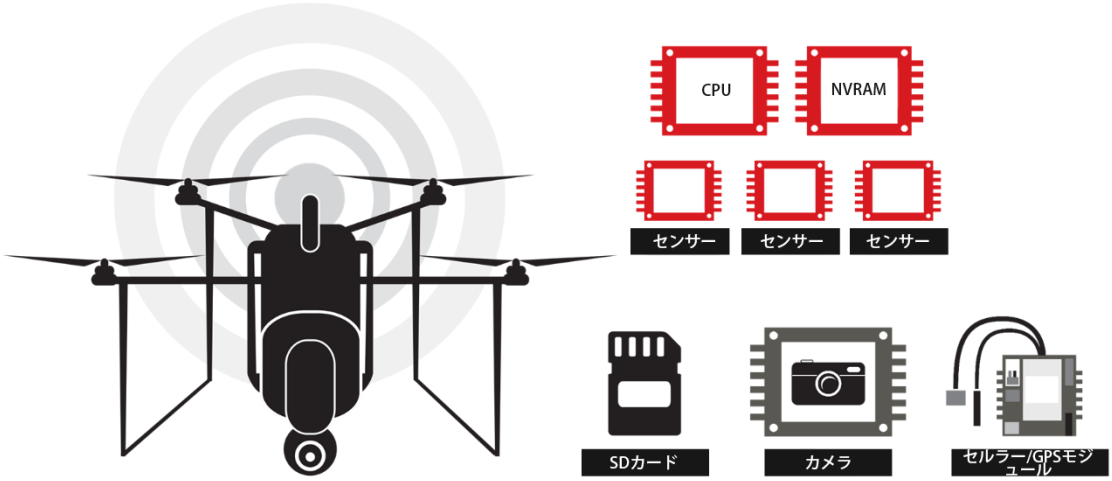


図 6 - ドローンとその主なコンポーネント

この個人用ドローンは、非常に頑強なコンポーネント群から構成されています。複数のモーター、センサーおよび全てが同時かつ効率的に機能する必要があるその他の機器を備えており、高い処理能力を発揮します。このモデルは、ARM Cortex-A8 CPU を使用し、主要オペレーティングシステム（Linux）は別のチップの NVRAM に保管されています。動作や光、速度などを検出するためには、さまざまな種類のセンサーが必要です。動画やセンサーメトリクス、メタデータを保存するのに SD/MMC カードが使用されています。カメラが搭載されており、操縦者はドローンの位置からの眺めを見ることができます。また、ドローンが専用プロトコルの範囲外にいてもドローンが操縦者との接続を維持できるよう、セルラー/GPS のコンビネーションモジュールが使用されています。GPS は、誘導や最低限の自動化のためにも使用されています。

動力にはリチウムポリマー（LiPo)電池が使用されています。全ての機能が同時に作動している場合、新たに充電が必要となるまでの飛行時間はおよそ 2 時間です。

エンドポイントエコシステムの文書によれば、このデバイスは複雑エンドポイントクラスに分類されるでしょう。セルラーモジュールを搭載してますが、他のエンドポイントとのメッセージのやり取りを行わないため、ゲートウェイとはみなされません。

## 9.2 サービスの概要

サービスの観点からみると、バックエンドが使用されるのは、ドローン飛行中に専用ラジオインターフェイスからの消失が検出された場合に操縦者と接続するために限られます。ドローンが飛行中にセルラーに接続できるようになっている場合、LTE ネットワークを通じて操縦者が接続するのを待とうとするでしょう。しかし、LTE による制御不能となった場合、最後に離陸した場所に自動的に着陸しようとします。

ただし、ドローンには簡単な自動機能が付いているため、写真や動画を撮影しながら、移動するための経路や座標を提示することができます。自動操縦の間、操縦者にドローンのコースや視点を見せるため、これらのメディアファイルは、リアルタイムでバックエンドサービスに LTE を通してアップロードすることができます。

このように、システムに接続されている各ドローンには、サービスの高い可用性を確保するために頑強なバックエンドサービスが必要となります。動画や高解像度の画像をセルラーリンクで転送するために、高いネットワークトラフィックのバーストに対する可用性も必要です。また、操縦者がウェブブラウザからアップロードされたメディアを見ることができるように、ウェブインターフェイスも必要となります。

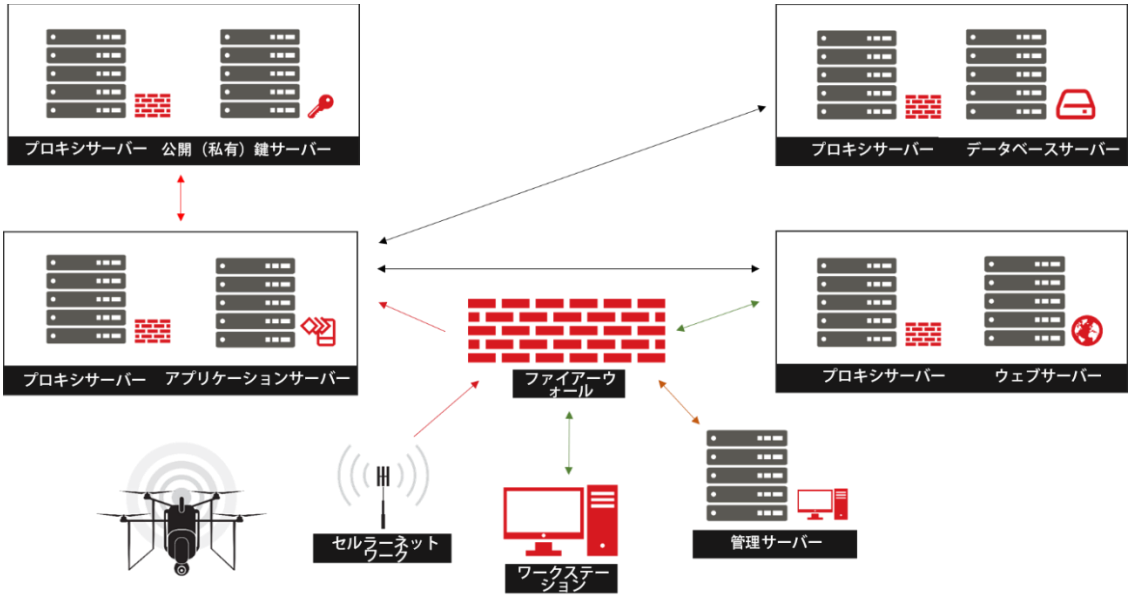


**図 7 - バックエンドサービスへのデータフロー**

## 9.3 使用例

この技術の開発業者は、エンドユーザーがドローンを自然環境での撮影に用いることを想定していました。しかし、価格の割にはカメラとドローンの静止機能が極めて高品質であったため、実際のドローンの利用客の一部は映画の撮影に利用しています。今後は高額の映画プロジェクトでも使用されることになるため、知的財産やプライバシーが主要な問題となるでしょう。

## 9.4 セキュリティモデル

この事例の企業のエンジニアリングチームは、自社の製品またはサービスに最も関係がある問題を特定するために、エンドポイントとサービスの文書の「セキュリティに関するよくある質問」セクションを活用しました。

その結果、エンドポイントの観点からは、以下のような問題点があることがわかりました。

- エンドポイント ID
- エンドポイントのなりすまし
- トラストアンカー攻撃
- ソフトウェアとファームウェアの改ざん
- セキュリティで保護されたリモート管理
- セキュリティ侵害を受けたエンドポイントの検出
- サービス上のなりすまし
- プライバシーの確保

一方、サービスの観点からは、以下の問題点を特定しました。

- ユーザーのプライバシーの管理
- 可用性の向上

チームは、関連する「セキュリティに関するよくある質問」セクションに従って、上記のそれぞれの問題に対する推奨事項を見直し、費用対効果が高く、最大のセキュリティを確保できる改善案の推奨事項を実装することにしました。

この事例のモデルでは、サービスのインフラストラクチャに大きな変更は必要ありません。というのも、エンドポイントでのサービス提供が膨大なトラフィックに耐えられるよう、サービスのインフラストラクチャは既に大幅に拡張されていたからです。このアーキテクチャは、単純に効率的に性能を上げるために、また何らかのサービスが一時的に機能しない場合でもリソースの可用性を維持するために、あらかじめ適切かつ安全な設計しておくことが必要でした。しかし、企業が予期しなかったニッチな利用方法に関するユーザーのプライバシーが大きな争点となっていたため、企業はさらに研究を進めることを決定しました。

一方、エンドポイントのインフラストラクチャには大きな変更が必要です。推奨事項に従って見直しを行った結果、エンジニアたちは重大な悪用リスクがあることに気付き、次のような問題を確認しました。

- ブートローダーは、オペレーティングシステムのカーネルを作動させる前にアプリケーションを正しく検証せず、改ざんのリスクにつながっている。
- アプリケーションやコミュニケーションのセキュリティを管理するために使用される TCB が無い。
- 適切に実装された TCB やトラストアンカーがないため、データの流出につながる恐れがあるエンドポイントのなりすましが問題となっている。
- 適切に実装された TCB なしでは、エンドポイントは正しくサービスを認証することができない。
- 適切に実装された TCB なしでは、エンドポイントは操縦者を専用無線インターフェイス上で正しく認証できない。
- エンジニアは通信チャネルがセキュリティ侵害を受けないようにするために LTE のセキュリティに依存してきたが、LTE のセキュリティを通り抜けて脆弱なサービスセキュリティを侵害をする、エンドポイントのなりすましやフェムトセルの用途変更の脅威を考慮していなかった。

## 9.5 結果

ガイドラインによって特定されたリスクに対して適切に対処できるように、上記の問題に関する推奨事項を実装したことで、企業のエンドポイントのアーキテクチャは大幅に改善されました。

既存のドローンシステムは既に生産されているため、エンジニアリングチームは、個人用パブキーセキュリティモデルを実装するファームウェアのアップデートを実施します。ファームウェアのアップデートは、コアアーキテクチャにセキュリティを導入するとともに、ブートローダーを改善します。個人用パブキーモデルが使用されたことから、他のユーザーのエンドポイントをなりすましながら、当初エンドポイントでセキュリティが不十分だったことを悪用しようとしても上手くはいかないでしょう。これは、エンジニアが既存のユーザーとエンドポイントのマッピングデータベースを利用して、ユーザーごとの個人用鍵を作成した

からです。これにより、適切なウェブ資格情報を持たないユーザーは、他のユーザーの個人用パブキーのアップデートをダウンロードしたり、インストールしたりすることができなくなります。このプロセスは複雑で、実装には時間がかかりますが、労力と時間を費やす価値はあるでしょう。

将来のドローン技術は、内部 CPU のトラストアンカーを実装することになるでしょう。このトラストアンカーは個人用パブキーの TCB に紐付けられています。これにより、各エンドポイントに独自の方法で優れたセキュリティを提供することができます。

このような方法で強力な暗号化を展開することは、企業が懸念する他の攻撃も無効にする可能性があるため、是非とも実行しなければなりません。強力な暗号化と、確認および認証のための TCB のメリットを活用すれば、エンジニアリングチームは、不正なサービスがドローンに通用するかどうかを簡単に検出することができます。不正サービスを検出した場合、ドローンは最初の離陸地点に戻ることができます。

セキュリティが不完全なドローンを検出するサービスも、内部信号を送信することができます。この場合、管理チームはセキュリティ侵害を受けた可能性のあるドローンをどのように処理するかを決めることができます。また、セキュリティに関する問題が起こった時の迅速性のレベルを確認でき、企業はエンドポイントの異常な動作の原因となっているソフトウェアやハードウェアを検証することができます。

### 9.6 要約

エンジニアチームは機械工学とバックエンドサービスの観点から、耐性の強いアーキテクチャを構築するために、非常に多くの時間を費やしました。また、安全なエンドポイント技術を開発するためには、非常に多くの作業が必要でした。今回の事例はビジネス全体に決定的な脅威を与えるものではありませんでしたが、お客様のニーズに*何とか応える*ことができるソリューションがあったことは幸運でした。もしこれが安全を脅かす可能性がある不十分な技術であれば、この事例で使用されたソリューションでも十分ではなかったでしょう。

個人用パブキーTCB、個人用 PSK TCB などのトラステッド・コンピューティング・ベース（TCB）の種類に関する詳細については、IoT サービスの文書[3]と IoT エンドポイントエコシステムの文書[4]を参照してください。

## 10 事例 - 車両センサーネットワーク

この事例では、本ガイドラインを使用して、新しい種類の自動車に搭載されている車両センサーネットワークを評価します。エンドポイントの評価はエンドポイントエコシステムの文書を使用し、サービスはサービスエコシステムの文書を使用して評価します。

### 10.1 エンドポイントの概要

まず、エンドポイントのハードウェア設計の評価から始めましょう。

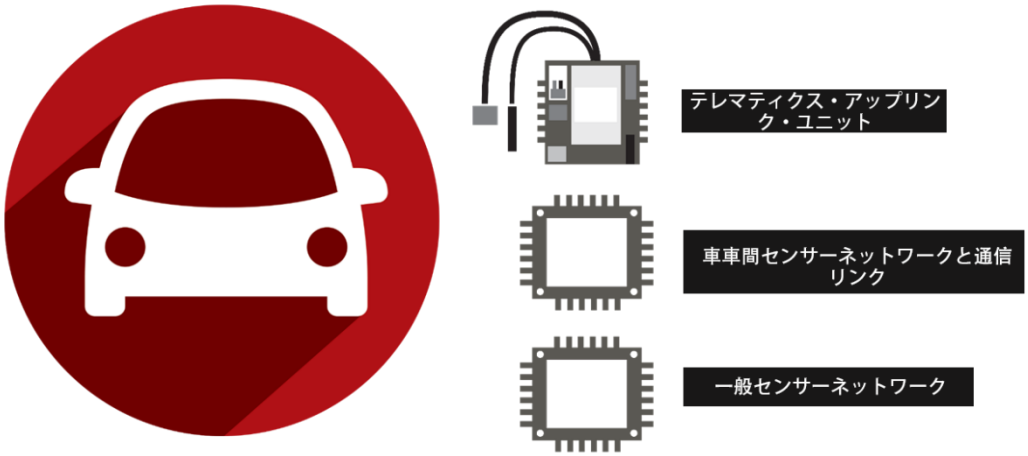


**図 8 - 完全車両センサーネットワークと通信システム**

上記のモデルは簡単な図では説明できないほど複雑なものですが、以下の 3 つの高水準のコンポーネントが含まれています。

- 運転手の代わりに複雑な意思決定を行い、バックエンドシステムとの接続を維持し、センサーネットワークを管理するテレマティクス・アップリンク・ユニット
- 車両対車両（V2V）のイベントを検出し反応する V2V システム
- テレマティクス・アップリンク・ユニットにメトリクスを提供する一般センサーネットワーク

現代の自動車システムでは、テレマティクス・ユニットは自動車コンピューターネットワークの一部であり、センサーデータとバックエンドとの通信に基づいて意思決定を行います。このユニットは、消費者である運転手とともに、または運転手の代わりに意思決定をします。このユニットが、車両を正しく作動させ、緊急事態には賢明な決断を下し、バックエンドネットワークからの指令を受けます。

V2V センサーネットワークは近くにいる車両を認識し、センサーから収集したメトリクスを基に意思決定を行います。コンポーネント（ブレーキやタイヤの空気圧モニターなど）の状態を基に、テレマティクス・ユニットが主に意思決定を行いますが、V2V システムも他の車両の存在に反応して意思決定を行ったり、重大な事象が発生した場合は近くの車両にアラートを送ります。

一般センサーネットワークは、テレマティクス・ユニットや、時には V2V ユニットにもデータを伝送するコンポーネント群です。これらのユニットは、重大な事象が発生した場合に正確な意思決定を行うために、一般センサーネットワークから収集した情報を利用します。

エンドポイントエコシステム文書によると、このシステムはあらゆる IoT のエンドポイントのクラスに適合するコンポーネントを備えています。テレマティクス・アップリンク・ユニットは、ゲートウェイとしての役割を果たしています。一方、V2V ユニットは複合エンドポイントの役目を果たします。一般センサーデバイスは、実質的には全て軽量エンドポイントです。

## 10.2 サービスの概要

サービスの観点からは、車両センサーネットワークはバックエンド環境にメトリクスを提供しています。このデータは、必ずしも消費者に提供されるとは限りません。このデータはむしろ、コンポーネントの潜在的な問題を監視または特定するために、製造業者が保管する可能性があります。これにより、サービス上の警告が発せられ、消費者に通告される場合があります。

またこのシステムは、消費者に「リモート・ドア・アンロック」や「エンジンスタート」などの便利なサービスを提供できるように拡張することもできます。近い将来には、自動ガイダンスシステムにより、車両の遠隔運転が実現するかもしれません。

ほとんどの重要な意思決定は、車両自体に搭載されたプロセシング・ユニットで行われますが、一部の意思決定がクラウド上でなされるようになることは十分考えられます。その場合、行動モデルや統計モデルを使用した機械学習（ML）や人工知能（AI）により、さらに複雑な意思決定ができるようになるでしょう。

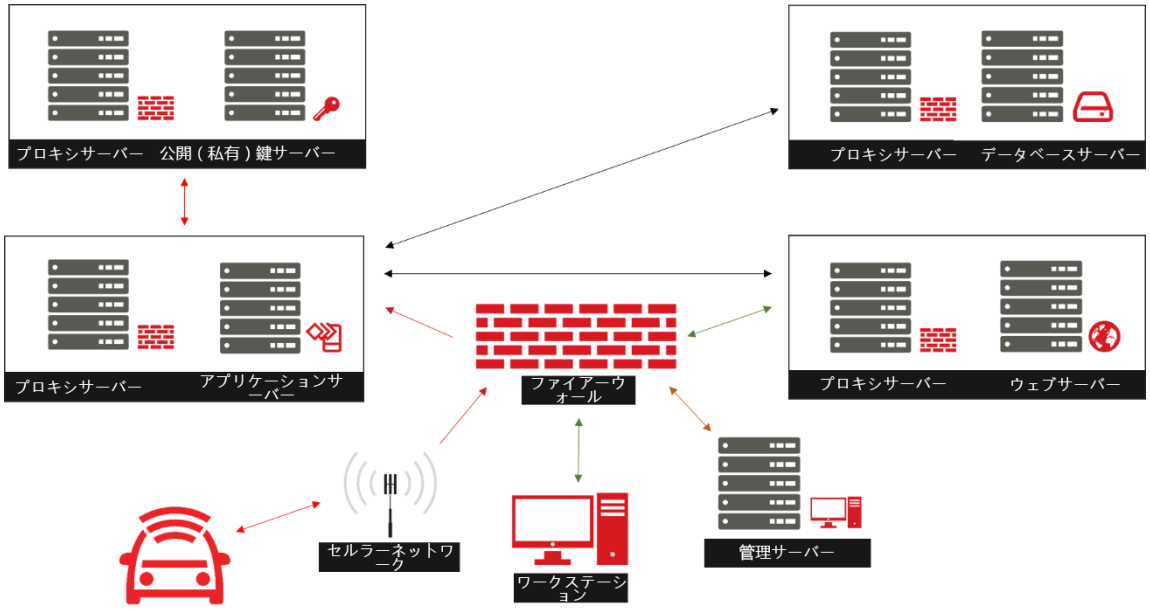


図 9- バックエンドサービスへのデータフロー

## 10.3 使用例

この技術の使用目的は明らかです。それは、安全性が最も重視される場合にも、複雑な意思決定ができるよりスマートな自動車を製造することです。できるだけ多くのセンサーのインテリジェンスを駆使して、短時間で重要な意思決定ができるようになることを目指します。自動ブレーキ、タイヤのパンクを知らせるブロードキャスト警告、一時的作動不能オペレーター警告の使用などの重大な危険を伴う状況でも、センサーの使用と綿密に設計されたコンピューターシステムによって解決できる可能性があります。

この技術の興味深い特徴の 1 つは、ユーザーに対して完全な透明性を確保できる可能性があるということです。ユーザーは、これらのコンピューターの設定を調整する必要はありません。その代わり、センサーのメトリクスを使用して、その時の状況に適切に対応できるようになる必要があります。これにより、コンピューターは周りの環境に関係なく正常に動作できることでしょう。

## 10.4 セキュリティモデル

この事例の企業のエンジニアリングチームは、自社の製品またはサービスに最も関係がある問題を特定するために、エンドポイントとサービスの文書の「セキュリティに関するよくある質問」セクションを活用しました。

その結果、エンドポイントの観点からは、以下のような問題点があることがわかりました。

- エンドポイントのなりすまし
- サービスまたはピアのなりすまし
- サイドチャネル攻撃
- セキュリティ侵害を受けたエンドポイントの検出
- セキュリティを犠牲にした安全確保

一方、サービスの観点からは、以下の問題点を特定しました。

- エンドポイントでの異常な動作の特定
- ユーザーのプライバシーの管理

この環境において、これまでの事例では説明されていない最大のリスクは、ピアのなりすましリスクです。このような環境下でエンジニアが懸念するのは、適切に認証されていないデータを使用してコンピューターが重要な意思決定を行ってしまうリスクです。

危険な状況でのセンサーのデータは迅速に処理することが要求されるため、理論的には非対称暗号化や PKI に基づく通信を実行することが常にできるとは限らないとされています。しかし、この主張は必ずしも正解ではありません。むしろ、時間が非常に重要な状況では、的確なセキュリティモデルを事前に準備し、近くのエンドポイントにセッションキーを隠しておくべきです。例えば、一定の速さで 2 つの物体が近づいている場合、サービスエコシステムのセキュリティアプリケーションは、2 つの物体がお互いに物理的に影響を与える距離に達する前に、これらの 2 つのエンドポイントに固有のセッションキーを準備することができます。これにより、危険な状況（自動車同士が衝突しそうになっている場合など）が発生する可能性が検出された際に、安全性が確保されたセッションで直ちに再ネゴシエートする時間がない場合でも、エンドポイントとセンサーの間で確実に安全な通信を行うことができます。

このように、TCB 実装には拡張が必要ですが、興味深いソリューションの 1 つとして GBA が挙げられます。GBA ではテレマティクス・アップリンク・ユニットに使用されている UICC が、システムを通してエンドポイントに鍵を安全に配布することができます。このプロトコルにより、多くの危険な状況において使用可能なセキュリティ保護済みのセッション

キーを、基本的なエンドポイントにも埋め込むことができるでしょう。このように、たとえ軽量エンドポイントが公開鍵セッション初期化に不可欠な演算ができなくても、常に信頼の基点に基づいた環境を確立することができます。

この環境においてもう 1 つ重要な問題は、セキュリティ侵害を受けたエンドポイントを検出することです。例えば、システム環境は、タイヤ空気圧モニター（TPM）などのシンプルなセンサーがセキュリティ侵害を受けていないかどうかをどのように認識するのでしょうか。コンピューターが、タイヤがパンクしているという TPM の情報に基づいて重要な意思決定を行った場合、安全性の問題が発生する可能性があります。そのため、デバイスを起動する際にデバイスの動作とその信頼性を毎回再評価する必要があります。全てのデバイスは耐タンパー性を備えている必要があり、セキュリティ侵害が発生した場合にネットワークに通知しなければなりません。逆に、センサーネットワークの他のデバイスが、ネットワーク上でピアの信頼性を評価できる方法もあるはずです。

## 10.5 結果

推奨事項を実行後、車両センサーネットワークは、車両通信ネットワーク上の攻撃に対してしっかりと保護されている状態となります。システム上全てのエンドポイントへの鍵配布に GBA が使用され、古い鍵が再使用されることがないよう、デバイスが起動されるたびに新しい鍵が配布されます。耐タンパー性、全てのエンドポイントにおける強力な TCB と組織の信頼の基点により、リスクが大幅に減少した環境が機能する状況が実現されました。

しかしこのような変更の後でも、安全性は依然として重要なファクターです。エンジニアリングチームと経営陣は、企業のリーガル（法務）チームや保険会社と協働し、安全性の鍵となる技術を評価し、ユーザーの安全を脅かすことなくセキュリティを実装できるかどうかを決めなくてはなりません。アーキテクチャの調整を行うことで、安全性が重要となる状況でもセキュリティを実装することは可能ですが、何を差し置いても安全性が最優先されなければならない場合もあります。

## 10.6 要約

多くの場合、このようなシステムは高度な技術を採用しているため、攻撃者がそのエコシステムに攻撃するには多大な努力が必要です。しかし、通信アーキテクチャの些細な欠陥が、セキュリティ侵害につながることもあります。CANbus ネットワークなどの閉鎖的な環境では、1 つのエンドポイントの欠陥がシステム全体を脆弱にしかねません。安全性が最優先されるべき環境では、これは許容できないリスクです。

# 付録 A　IoT サービス提供者向けに推奨されるプライバシーの考慮事項

GSMA では、IoT エコシステムで信頼性を確立し、規制当局からの公的な介入を最小限に抑えるため、以下のようなプライバシーリスクを最小限に抑える高水準のステップガイドを提案しています。IoT サービス提供者は、IoT 製品やサービスの初期の開発段階でこれらのステップに従いながら、質問事項を検討することが推奨されます。

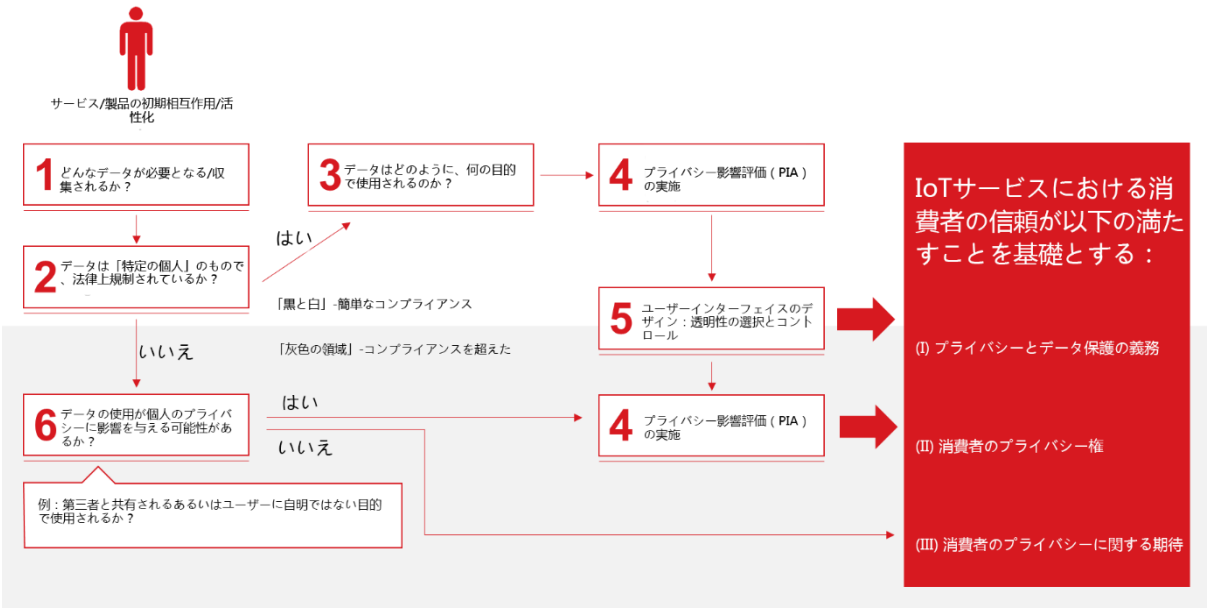


**図 10- 設計決定木による GSMA IoT プライバシー**

| ステップ | 考慮事項 |
|---|---|
| **ステップ 1** | **IoT サービスまたは製品が適切に機能するために、ユーザーから、またはユーザーについてどんなデータを収集する必要があるのか。**<br>データに依存するビジネスモデルの最初のステップの 1 つは、製品やサービスが適切に機能するために、消費者から、または消費者についてのどのような情報が必要なのかを特定することです。サービスが必要とするデータの種類は、静的なデータ（消費者の名前や自宅住所など）と動的なデータ（リアルタイムの所在地）に分類することができます。例えば、歩行数や消費カロリーを記録するフィットネスリストバンドを販売する場合、リストバンドを使用する人の体重や年齢、性別、移動した距離、心拍数などを知る必要がありますが、その人が実際にどこにいるかに関する情報は必ずしも必要ではありません。<br>必要なデータの種類を特定するにあたり、データの使用許可を該当する個人から得る必要があるかどうか、どのように同意を得るのか、さらには消費者自身がプライバシー設定を管理する選択肢をどのように提供するのかを決めなくてはなりません。製品自体に画面がない場合、ユーザーにプライバシーの選択肢を与えるメディアとして、（モバイルアプリやオンラインダッシュボードなど）スマートフォンを使用することもできます。 |

| | |
|---|---|
| ステップ 2 | **データは「特定の個人」のもので、法律上規制されているか。**<br>次のステップは、法律で規制されているデータ保護とプライバシー要件を特定することです。検討すべき質問事項は下記の通りです。<br>• 対象となる国や市場での「特定の個人」データの定義はどうなっているのか。<br>• 収集されたデータは「特定の個人」のもので、法律上規制されているか。もしそうであれば、そのようなデータを使用できる法的な根拠は特定できたのか。<br>• プライバシーに関連するライセンス規制の対象となっているか（電気通信事業者など）<br>• 一般的なデータ保護法以外に、提案するデータ収集モデルに関して、下記のような国や地方、業界固有の法律や規制はないか。例：<br>o 金融/決済サービス、医療業界の規制<br>o 国境を越えたデータのやり取りに対する規制の可能性 |
| ステップ 3 | **データはどのように、何の目的で使用されるのか。**<br>法律上の要件を満たす内容を確定した後、その次のステップは、収集したデータを使用して効果的なサービスを提供するために、それらをどのように使用するのか、誰と共有するのかを綿密に計画することです。データの取り扱いに関してセキュリティとプライバシーの両者を検討するには、以下のような質問が役立つでしょう。<br>• データが保存および伝送される際に、データの安全性が確保されているか。<br>• データフローを明確に設定したか。つまり、バリューチェーンの中で、どのように、どのような目的でデータが使用され、共有されるかを特定したか<br>• 予定しているサービスを提供するにあたり、それぞれの種類のデータの正当な必要性を説明できるか。<br>• 事前にビジネス上のパートナーと、プライバシーの責任について定義し、合意しているか（また、製品設計はその責任を反映しているか。）<br>• 消費者のデータを共有する企業と、適切な契約上の合意がなされているか。（アナリティクスの提供者が自社の商売上の理由でデータを使用することへの制限など）。このような契約書または制限事項は 2 社間の合意に基づいたものにするか、または契約違反が発覚した場合の義務と責任を明確に定めた行動規範もしくはガイドラインを自社で策定し、ビジネスパートナーにそれを遵守するよう求める。 |

| | |
|---|---|
| ステップ 4 | **プライバシー影響評価の実施**<br>プライバシー影響評価（PIA）の実施には、以下の項目が含まれます。<br>• 製品やサービスに個人のプライバシーに関するリスクがある場合、それが何かを特定する。<br>• 個人情報の誤用・悪用から生じる、個人に対する損害リスクを軽減する。<br>• 個人データの取り扱いに関して、より効率的かつ効果的なプロセスを設計する。<br>データ保護とプライバシーに関する法律で、PIA の要求は常識になりつつあります。英国の Information Commissioner’s Office（ICO）による出版物[10]や、International Association of Privacy Professionals による出版物など、多くの PIA の実施方法に関するガイドが公開されています。<br>PIA を実施する際の典型的な質問事項には、下記のようなものがあります。<br>• プロジェクトの実施により、自社またはパートナーの意思決定や行動が、個人に大きな影響を及ぼすのか。<br>• 健康状態や犯罪歴など、一般的にプライベート情報だと考えられる個人に関する特定の情報が、プライバシー上の懸念または期待を引き起こすことになるか。<br>• プロジェクトでは、プライバシーを侵害していると感じさせるような方法で個人に接触する必要があるか。 |
| ステップ 5 | **ユーザーインターフェイスでのプライバシーに関する設計**<br>消費者に対するプライバシーリスクを評価した後、そのようなリスクに対する消費者の認知度を引き上げる方法、リスクを緩和する方法、および消費者に対してプライバシーに関する選択肢を提示する方法を考えなければいけません。つまり、このステップはユーザーフレンドリーな方法で法律上の義務と消費者のニーズや期待に応えるサービスを確実に提供するためのものであり、プライバシーをしっかり管理できるという保証を与えることで、消費者の信用を勝ち得ることを目的としています。検討すべき質問事項は下記の通りです。<br>• 消費者がどのようにプライバシーのリスクに気付き、提示された選択肢を選ぶことができるのか。<br>• 法律上必要とされる場合に、消費者の同意を取得したか。同意に含まれる重要な要素は、開示、理解、任意性、適正および契約です）<br>• 伝送および保存中のデータに対する安全性は確保されているか。<br>• 消費者データの保存期間は決められているか（またその理由は何か）。<br>• カスタマージャーニーは、下記のような消費者の信用獲得に役立っているか。例：<br>o 消費者は、享受するサービスと引き換えにどのようなデータが共有されているのかを理解しているか。<br>o 消費者は、ウェブベースの「権限ダッシュボード」、「ジャスト・イン・タイム」プロンプト、コールセンター、モバイルアプリ、音声コマンドなど、簡単な手順でプライバシー設定を管理することができるか。 |

| | |
|---|---|
| **ステップ 6** | **データの使用が個人のプライバシーに影響を与える可能性があるか**<br>製品やサービスで収集するデータは、法律上必ずしも「特定の個人」のものとは言えないものかもしれませんが、早期に検討するべきプライバシー関連の懸念はまだ残っています。関連するデータが消費者のプライバシーに影響を与えずに使用できるかどうかを確認するために、以下の点を考えてみましょう。<br>• 提供するサービスや製品からの（特定の個人のものではない）データが、他のソースから得られたデータと組み合わせることにより、消費者の個人的な生活に関する情報を推測できる可能性はあるか。個人のライフスタイル、習慣、宗教などについて推測される情報は、下記に該当するか。<br>o 健康保険の契約能力に影響を与えないか。<br>o 第三者（小売業者、保険会社など）が、特定の消費者に対して差別的な価格を提示することに使用されることはないか。<br>• 提供する製品やサービスが将来のある時点で変更される場合、その変更が消費者に与える影響にはどのようなものが考えられるか。例：<br>o 変更することで、消費者についての新しい情報（位置情報など）を収集することになるのか。<br>o 当初の取得目的とは異なる目的で消費者データの使用を考えている第三者（広告業者など）に、既存・新規の消費者データが共有または売却されていないか。<br>• 製品やサービスを変更する場合、以下の対応を行う必要があります。<br>o 変更によって新しい法律が適用される場合の事業への影響を確認する。<br>o 消費者への通知プロセスを確立し、必要に応じて本人の同意を得る。<br>o 消費者にプライバシー設定を変更する手段を与える。<br>• 上記に加えて、IoT のサービス提供者は下記の対策を検討することが推奨されます。<br>o バリューチェーン上の各パートナーの責任を明確化するよう、適切な契約を確実に締結する<br>o 問題が発生した場合や消費者がプライバシー侵害を受けた場合、消費者向けの相談窓口の設置を含む、明確な是正プロセスを策定する |

下の図は、上記に提案したステップを説明するための一案です。

# 付録 B　自動車追跡システムに関する事例

この事例では、IoT セキュリティ・ガイドラインを使用して、自動車追跡システムを評価します。このプロセスは、本概要説明書のセクション 6「本ガイドラインの有効な使い方」を補足するものです。

## A.1　テクニカルモデルの評価

最初のステップは「テクニカルモデルの評価」です。エンジニアリングチームは、デバイスが製品のアーキテクチャに基づいてどのように機能するのかを評価します。人選とセキュリティタスクの割当、進捗管理のために、ソリューションに使用される技術を項目別に示した文書を作成します。

説明を簡単にするため、自動車追跡システムは以下のような機能を持つものとします。

- **エンドポイントのエコシステム：**
  - シンプルなグラフィック・ユーザー・インターフェイス（GUI）により、ユーザーは以下を行うことができます。
    - ユーザー名とパスワードを使用したログイン
    - 追跡の無効化
    - 追跡の有効化
    - 現在位置の確認と視覚化
  - バックエンドサービスへの接続のためセルラーモジュール
  - セルラーモジュール用の SIM カード
  - バックアップ電源用のリチウムポリマー電池
  - 中央処理装置（CPU）
  - 不揮発性 RAM 内の埋め込みアプリケーション
  - RAM
  - EEPROM

- **サービスのエコシステム：**
  - セルラーデータの接続性
  - 保護されたプライベート APN
  - サービスのアクセスポイント
  - セルラーモデム OTA 管理サービス
  - SIM カード OTA 管理サービス

それぞれの技術に関連する情報を確認した後、チームで各ガイドライン文書の「モデル」セクションを見直し、適切なテクニカルモデルを特定します。このエンドポイントは複合エンドポイントにあたります。サービスとネットワークモデルは、標準的なモバイル対応 IoT サービスです。

## A.2　セキュリティモデルの見直し

テクニカルモデルの概要を決定した後、企業はセキュリティモデルの見直しのステップに移行することができます。セキュリティモデルでは、攻撃者がどのようにソリューションを攻撃するかを見極めます。

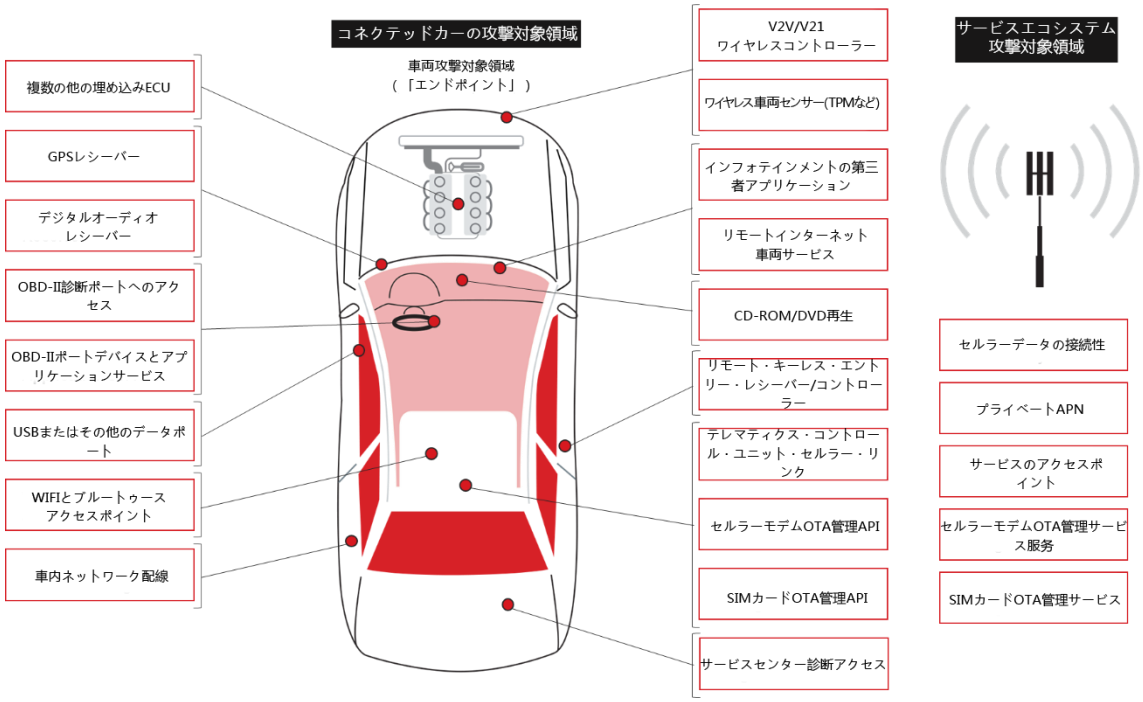


**図 11 - コネクテッドカーの攻撃対象領域**

このソリューションの例では、攻撃の恐れがある外部からのアクセスポイントは 2 か所しかありません。

- セルラーネットワーク
- 車両へのローカル攻撃

ローカルネットワークとの接続ではなく、モバイルネットワークとの接続なので、攻撃者はセルラーネットワーク接続からセキュリティ侵害を行い、プライベート APN から通信チャネルに侵入するか、サービスアクセスポイント、セルラーモデム OTA 管理サーバー、または SIM カード OTA 管理サーバーを経由して侵入するしかありません。

これ以外に考えられるのは物理的なデバイスへのセキュリティ侵害ですが、上の図からわかるように、多くのエントリーポイントがあるので、この IoT サービスの場合はエンドポイントに焦点を当てる必要があります。

## A.3　セキュリティタスクの見直しと割り当て

セキュリティモデルの評価が完了すると、セキュリティタスクを容易に割り当てることができます。各チームは、評価が必要なソリューションのコンポーネントに対して、特定の担当者を割り当てる必要があります。専門的な観点（エンドポイント、ネットワーク、サービス）からだけではなく、サブコンポーネントの観点からも評価を行う必要があります。つまり、CPU は作業者やオペレーティングシステム、ネットワークサービスなどに割り当てられなければなりません。

各コンポーネントの担当者が決まると、プロセスを開始することができます。この段階では、チームは以下の点を理解している必要があります。

- 技術の構造はどうなっているか
- セキュリティに影響を与える技術は何か
- 特定の技術を有しているエンジニアリングの関係者は誰か

## A.4 推奨事項の見直し

「推奨事項の見直し」段階では、チームの各メンバーは*少しでも多くの*推奨事項を読んで理解しておく必要があり、計画にしっかり組み込んでおくことが不可欠です。特定のコンポーネントに関連した推奨事項のみを重視するのではなく、それぞれのコンポーネントが全体の製品やサービスのセキュリティにどのように影響を与えているのかについての理解を深めるために、エンジニアはできるだけ多くの推奨事項、特に専門性の高いものを時間をかけて理解する必要があります。こうすることで、費用対効果、寿命、管理の観点から最もバランスのとれた是正または緩和戦略について、グループ全体で有意義な議論をすることができるのです。

*コンポーネントの担当者*は、推奨事項を見直した後、推奨事項が既に適用されているかどうかを確認し、推奨事項を*保留する*かどうかを決定することができます。これにより、実際に展開する前に、グループで推奨事項の適用性について改めて議論することができます。推奨事項によっては、他の推奨事項や既存の管理に悪影響を与える可能性もあるため、これは望ましい戦略と言えます。

この事例では、チームは以下の点を決めることになるでしょう。

- アプリケーションのトラスト・ベースの使用
- 組織の信頼の基点の定義
- デバイスパーソナリゼーションの実行
- 耐タンパー性のある文字種の実装
- エンドポイントのパスワード管理の強化
- エンドポイントの通信セキュリティの強化
- 暗号署名画像の実装
- プライバシー管理の実行
- デバイス電源アラートの統合

## A.5 コンポーネントのリスクの見直し

次に、各コンポーネントを製品またはサービスに実装または統合する際の様々なリスクを特定するために、「コンポーネント」セクションに従ってリスクを評価する必要があります。作業を最小限に抑えるために、通常このセクションはコンポーネントの担当者のみが見直しを行いますが、担当者以外のメンバーもできるだけ多くの項目に目を通すことが推奨されます。

推薦事項とコンポーネントの「リスク」セクションを見直した後、以下のようなセキュリティギャップが確認されました。

- 機密情報は EEPROM 内で保護されずに保存されていた
- 機密情報は内部 RAM 上で処理されていなかった
- ユーザーインターフェイスはパスワードを保護しなければならない
- ユーザープライバシーの概要はユーザーに説明されるべきである

## A.6 実装と見直し

次に、チームは同意したセキュリティ推奨事項に従って、ソリューションを修正する必要があります。必要に応じてコンポーネントを再実装し、セキュリティコントロールを追加しなければならないでしょう。

この事例では、チームと協働する GSMA の担当者がアプリケーションで動作するトラストアンカー技術を含有した SIM カードを提供できることが判明したため、既存の SIM カードを利用することでトラストアンカーに対するニーズは満たせるでしょう。また、各 SIM カードは GSMA の標準的な技術を使用して現場でパーソナライズできるため、パーソナリゼーションの問題も解決します。

また SIM 技術は、OTA で通信セキュリティを提供することもできるため、プライバシーと通信認証実装のニーズも解決してくれます。

SIM の企業固有ゾーンはトラステッド・ルート・ベースにプログラムすることが可能で、企業は証明書チェーンを使用してピアの認証を行うことができます。これにより、組織の信頼の基点とピア認証要件の問題を解決することが可能です。

製品梱包は、適切な耐タンパー性のあるパッケージに変更されています。

EEPROM は、SIM のトラストアンカーに保存されているセキュリティーキーで暗号化されたデータによってエンコードされます。

ブートローダーはアプリケーションイメージの認証のためにトラストアンカーを使用するよう変更されます。

エンドポイントは、タイプされたパスワードの文字をブロックアウトし、ユーザーによって入力されたパスワードの安全性の確保をサポートするようプログラムし直されます。

プライバシーを管理する GUI が追加され、ユーザーは企業がどのような情報を収集するかを確認し、管理することができます。

機密情報は同じチップの内部メモリ内だけで処理されます。

実装内容が定義されると、チームは全ての推奨事項とリスクを改めて評価し直し、変更内容が懸念事項を解決したかをどうかを確認するため、セキュリティモデルを見直します。

## A.7 ライフサイクルの継続

承認を受けた構成が完成したので、チームはこの段階で技術を展開することができます。しかし、セキュリティ対策はここで終了するわけではありません。エンドポイントのセキュリ

ティのアノマリー監視方法と、使用中の技術が新たに発見されたセキュリティギャップを有しているかを確認する方法を、チームで話し合って決定します。

また、それぞれのインシデントやギャップを特定および是正し、そこから回復する方法に関する計画を立てます。これにより、今後もますます進化する技術とセキュリティ環境が予期せぬ悪影響を企業に及ぼすことを防ぐことができるでしょう。

# 付録 C　　文書管理

## A.8　文書の履歴

| バージョン | 日付 | 変更事項の簡記 | 承認者 | 編集者/会社名 |
|---|---|---|---|---|
| 1.0 | 2016 年 2 月 8 日 | New PRD CLP.11 | PSMC | Ian Smith<br>GSMA<br>&<br>Don A. Bailey<br>Lab Mouse Security |
| 1.1 | 2016 年 11 月 7 日 | GSMA IoT セキュリティ評価スキームの参考資料の追加。<br>軽微な修正。 | PSMC | Ian Smith<br>GSMA |
| 2.0 | 2017 年 9 月 29 日 | LPWA ネットワーク情報の追加と軽微な変更。 | IoT Security Group | Rob Childs<br>GSMA |

## A.9　その他の情報

| 種類 | 説明 |
|---|---|
| 文書の所有者 | GSMA IoT プログラム |
| 連絡先 | Rob Childs - GSMA |

GSMA は、お客様に高品質の情報をお届けしたいと考えています。誤記や記載漏れなど、お気づきの点がございましたら、ご意見をお寄せください。お問い合わせ先：
prd@gsma.com

ご意見、ご提案、ご質問をお待ちしております。