



IoTセキュリティガイドライン 概要説明書

2016年2月

IoT セキュリティガイドライン概要説明書」

バージョン 1.0

2016 年 2 月 8 日

本文書は GSMA の拘束力のない永久参照文書です。

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 GSMA 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、GSMA 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し、またはそれ以外の方法で利用させることを禁じます。

著作権表示

Copyright © 2016 GSM Association

免責事項

GSM Association (GSMA) は、本文書に記載する情報の正確性または網羅性または適時性について、(明示、黙示を問わず) 一切の表明や保証、約束をおこなわず、それらに対する責任を本免責条項によって放棄します。本文書の情報は予告なしに変更されることがあります。

反トラスト法上の通知

本文書の情報は、GSM Association の反トラスト法順守方針を全面的に順守しています。

内容

1	はじめに	5
1.1	概要	5
1.2	GSMA の IoT セキュリティガイドライン文書セット	6
1.3	文書の目的	6
1.4	想定読者	7
1.5	用語の定義	7
1.6	略語	9
1.7	参照資料	10
2	モノのインターネットがもたらす課題	11
2.1	可用性に関する課題	12
2.2	ID に関する課題	13
2.3	プライバシーに関する課題	13
2.4	セキュリティに関する課題	14
3	モバイルのソリューション	15
3.1	可用性の課題への対処	15
3.2	ID に関する課題への対処	16
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	17
4	IoT モデル	17
4.1	サービスのエコシステム	18
4.2	エンドポイントのエコシステム	19
5	リスク評価	19
5.1	目標	20
5.2	参照リスクモデル	21
6	プライバシーの検証	21
7	このガイドラインの有効な使い方	24
7.1	テクニカルモデルの評価	24
7.2	現在のセキュリティモデルの見直し	25
7.3	推奨事項の見直しと評価	26
7.4	実装と見直し	27
7.5	ライフサイクルの継続	27
8	実例 — ウェアラブルの心拍数モニター	28
8.1	エンドポイントの概観	28
8.2	サービス概観	29
8.3	使用例	30

8.4	セキュリティモデル	30
8.5	結果	32
8.6	要約	33
9	事例 – 個人使用のドローン	33
9.1	エンドポイントの概観	33
9.2	サービスの概観	34
9.3	使用例	35
9.4	セキュリティモデル	36
9.5	結果	37
9.6	要約	38
10	事例 – 車両センサーネットワーク	39
10.1	エンドポイントの概観	39
10.2	サービスの概観	40
10.3	使用例	41
10.4	セキュリティモデル	41
10.5	結果	43
10.6	要約	43
付属資料 A	IoT サービス提供者向けに推奨されるプライバシーの検証	44
付属資料 B	自動車追跡システムに関する事例	50
B.1	テクニカルモデルの評価	50
B.2	セキュリティモデルの見直し	51
B.3	セキュリティタスクの見直しと割り当て	52
B.4	推奨事項の見直し	52
B.5	構成要素のリスクの見直し	53
B.6	実装と見直し	53
B.7	ライフサイクルの継続	55
付属資料 C	文書管理	55
C.1	文書の履歴	55
C.2	その他の情報	55

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生まれています。アナリストの予想によると、今後十年で多くの新しいIoTサービスによって何十億もの新たなIoT機器が接続される見込みです。新たなエコシステムのすべての参加者にとって、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です。

新しいIoTサービスが数多く展開されるにあたっては、セキュリティの問題が重大な阻害要因になると同時に、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度合いが増大する懸念をアナリストは指摘しています。この分野に攻撃者が関心を深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って、サービスに対する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開発してなかったり、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緩和するためのスキルと専門知識を利用できる態勢がなかったりするかもしれません。一方の敵対者は、技術とセキュリティの弱さを熟知しており、脆弱性が発覚すればすぐに付け込めます。

自動車、ヘルスケア、消費財、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、自分たちの市場に固有の特殊なセキュリティが必要と考えていますが、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・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機器とサービスプラットフォームの構成要素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に考え得るソリューションは、概して非常に似通っています。

GSMA が代表する電子通信業界には、顧客に安全性の高い製品・サービスを提供してきた長い歴史があります。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関連事業者と共に、セキュリティに関するその専門知識を、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、この一

連のセキュリティガイドラインを作成しました。

1.2 GSMA の IoT セキュリティガイドライン文書セット

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 のセキュリティの問題に対する共通の理解の確立にあたって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確実にするために、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、一連の文書において、IoT サービスにおける一般的なセキュリティへの脅威と弱点を軽減する方法についての推奨要件を説明しています。

以下の図は GSMA セキュリティガイドライン文書セットの構成を示すものです。本文書（本概要説明書）を手引きとして目を通した後に、その他の関係文書へと読み進めることをお勧めします。

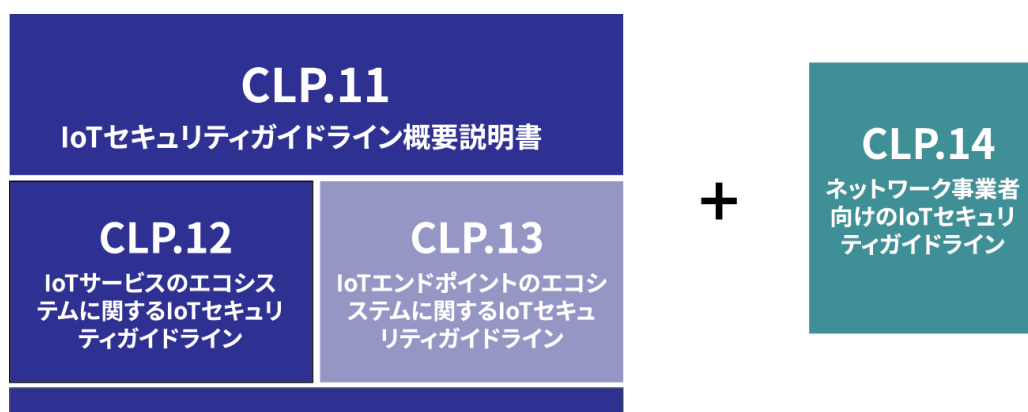


図 1 : GSMA 「IoT セキュリティガイドライン文書」の構成

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、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]に目を通す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確実にするための最高位のセキュリティガイドラインを示したものです。

1.3 文書の目的

IoT セキュリティガイドライン文書セットの目的は、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示すことにあります。こ

の目的上、本文書はどの側面が実装者に関連する技術またはサービスなのかを説明する、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構成要素を特定することにより、実装者は各構成要素に関連するリスクを評価し、その補正方法を決定することができます。また、それぞれの構成要素をサブ構成要素に分解し、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、修復のコスト、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。

本文書は、あくまで IoT サービスの設計と実装に関する推奨の範囲に限定されます。

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する意図はありません。

特定の地域の国内法令を必要に応じて順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は多数にあるが、その中には、スマートホーム、スマートシティ、自動車、輸送、ヘルス、公益事業、家電が含まれる。
- IoT 機器製造業者—IoT サービス提供者向けに IoT サービス対応の IoT 機器を提供する業者
- IoT 開発業者—IoT サービス提供者向けに IoT サービスを構築する業者
- ネットワーク通信事業者—自らが 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	エンドポイント機器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、多くの場合、ネットワーク事業者別に設定される。

攻撃者	一般的には情報の取得や破壊、制限、改ざんの意図により、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、処理をおこなう、インターネット上にあるリモートサーバのネットワーク。
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への継続的な接続性を備えたエンドポイントの 1 モデル。詳しくは CLP.13 [4]を参照。
構成要素	CLP.12 [3]と CLP.13 [4]にある構成要素の説明を参照。
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、ゲートウェイその他の接続機能を備えたデバイスの総称。詳しくは 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、複雑度の低いデバイス、リッチデバイス、ゲートウェイからなる構成。詳しくはセクション 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機械、機器、器具が協調して動作することをいう。このデバイスには、タブレットや家電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、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 機器からのデータを活用するコンピューターのプログラム。
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組織。
ネットワーク事業者	IoT エンドポイント機器を IoT サービスのエコシステムに接続する、通信ネットワークの運営者および所有者。

信頼された組織的なルート	ID、アプリケーション、コミュニケーション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続。
推奨要件	CLP.12 [3] と CLP.13 [4]に説明のある推奨要件を参照。
リスク	CLP.12 [3]と CLP.13 [4]にあるリスクの説明を参照。
セキュリティタスク	CLP.12 [3]と CLP.13 [4]にあ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 サービス提供者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のに必要とされる、一連のサービス、プラットフォーム、プロトコルその他の技術。詳しくはセクション 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 TS1 02 221（欧州電気通信標準化機構の技術仕様）に規定のある、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 に規定のある、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 プロセス 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	電氣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 インターフェース
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 (LPWA)
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
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 参照資料

参照	文書番号	タイトル
[1]	該当なし	「モバイルエコノミー 2015」 http://www.gsma-mobileeconomy.com/
[2]	SGP.01	「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」 http://www.gsma.com/connectedliving/embedded-sim/
[3]	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 www.gsma.com/connectedliving
[4]	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 www.gsma.com/connectedliving
[5]	該当なし	NIST リスク管理フレームワーク www.gsma.com/connectedliving
[6]	CMU/SEI-2007-TR-012	OCTAVE Allegro の導入： 情報セキュリティに関するリスク評価プロセスの改善に向けて http://www.cert.org/resilience/products-services/octave/

[7]	未使用	未使用
[8]	TS 33.220	汎用認証アーキテクチャ（GA）、汎用ブートストラッピング アーキテクチャ（GBA） www.3gpp.org
[9]	RFC 4186	汎欧州デジタル移動電話方式（GSM）向けの拡張認証プロトコルの加入者識別モジュール（EAP-SIM） www.ietf.org
[10]	該当なし	プライバシー影響評価の実施に関する実務指針 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[11]	該当なし	オープン・モバイル・アライアンス http://openmobilealliance.org/
[12]	該当なし	oneM2M http://www.onem2m.org/
[13]	CLP.14	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 www.gsma.com/connectedliving
[14]	GE.11-1320 1	意見および表現の自由に対する権利の促進と保護に関する特別報告担当者によるレポート（Frank La Rue*） www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	該当なし	インターネットへのアクセス権 https://en.wikipedia.org/wiki/Right_to_Internet_access

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・技術的变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ひとつでありながら、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呼応して、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」と技術者は十年前から言っていたものの、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折り合って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構成要素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しました。

つまり、これこそが「モノのインターネット」なのです。IoT 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もはや別個のものではなく、両者はますます強くつながっています。

そして、人間の身体的な経験がかつてないほどデジタル世界につながれ、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、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一段と充実させ、イノベーションの爆発を生じさせるという目標に向けて、全世界の人びと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とするには、それらの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： システムの整合性が確認・追跡され、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、エンドポイント機器がお互いに、さらにエンドユーザーやバックエンドのサービスと、常時情報をやり取りできなくてはなりません。その実現には、持続的な接続を可能にする新技術を考案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、以下の問いの答えを明らかにしなくてはなりません。

- 最新のセルラーシステムに対し、いかにしてセキュリティ水準が同程度のローパワー ワイドエリア ネットワーク（LPWAN）を実装することができるか。
- 新規の 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トラスト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ばよいか。

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作動するには、エンドポイントはピア端末とサービスに対して自己を確実に識別できなくてはなりません。この IoT 技術の重大かつ基本的な性質によって、サービスとピア端末によるデータの配信先の保証が確保されるのです。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問われるべきです。

- 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。
- サービスとピア端末は、エンドポイントの ID を確認することによって、いかにしてエンドユーザーの ID を確認できるか。
- エンドポイントのセキュリティ技術による、ピア端末とサービスの認証は可能か。
- 承認のあるサービスとピア端末を、不正なサービスとピア端末が偽装することは可能か。
- 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。

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・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アクション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がデザインされ、一切のアクションが承認を受け、すべての ID が確認されるようにしつつ、アクションとそれに関連するメタデータが権限のないパーティ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。その実現は、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、遡及的におこな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、人間のフィジカルな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・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。

したがって、プライバシーがエンドユーザーにいかに関与するだけでなく、次のような IoT 技術の設計方法についても自問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、アクション、スリープ中か活動中かなどの状態）を示唆したり、それに直接関連付けられていないか。
- 作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整合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。

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 技術の二大構成要素である、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。

- 信頼計算処理ベース（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つき、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分割するか。
- 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。

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、安全かつ費用効率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、分析モデルが生まれました。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不正使用や ID の乗っ取り、不正が生じる可能性を減らす取り組みがおこなわれてきました。

3.1 可用性の課題への対処

GSMA の「モバイルエコノミー 2015」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、2014 年末の時点でユニークモバイル加入者は計 36 億人に達している。10 年前にはモバイル加入者は世界人口の 5 人に 1 人に過ぎなかったが、現在では世界人口の半分がモバイルに加入済みで、この数は 2020 年までにもう 10 億人増え、全世界のモバイル普及率は約 60%に達すると予想されている。全世界での SIM 接続件数は 2014 年末の時点で 71 億件、それ以外に M2M 接続が 2 億 4300 万件だった。
- 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、2014 年末の時点では総接続数の 40%に満たなかったが、2020 年までにほぼ 70%に増加するとみられる。

- 2G は現在のところ世界の主要なネットワーク技術にとどまっているが、その地位はすでに著しく低下している。2G 接続は 2008 年には全体の 90%を占めたが、2014 年末の時点では 60%前後に低下した。2G 接続数だけをみると、2013 年にピークを迎え、2014 年には 6% 減少した。
- より高速のネットワークへと技術が絶えず移行する背景には、事業者による多額の投資がある。GSMA の最近の調査によると、3G ネットワークへのアクセス率は、現在の 70%から、2020 年には 5 人中 4 人を超える割合となると予想される。同報告書ではまた、3G を上回るペースでの 4G ネットワークの拡大が指摘されている。3G ネットワークが世界人口の半分にまで普及するのに 10 年かかったが、4G ネットワークは運用開始からわずか 8 年の 2017 年には同様のレベルに達する。

今後は、ローパワー ワイドエリア ネットワーク（LPWA）のワイヤレス技術をセルラー通信スペースへ組み込んで、IoT のニーズに対処する動きも見られるでしょう。この種の通信技術によって、現代のモバイルネットワークは、有効な通信をおこなうのに必要となるわずかな電力で、広域をカバーするワイヤレスの接続が可能になります。近い将来、移動体通信事業者は自社のサービスとビジネスに対するソリューションの提供に、LPWA のプロトコルと技術を取り入れることになるでしょう。

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、それによって、下位の構成要素レベルでのエンドポイント機器への組み込みや、製造コストの削減、全耐用期間にわたって IoT エンドポイント機器の接続を有効にする、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。それは、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さらに一層の素晴らしい進歩は、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あったことを意味します。これらの技術には二重の用途があります。ネットワークのセキュリティの検証だけでなく、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それ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]等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。

これらの技術を併せて用いると、現在の複雑なエンジニアリング プロセスは容易になり、ひとつの単純な構成要素にまとめられます。アプリケーション エンジニアが自分で管理する必要の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 を予め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、不正その他の悪質な行為の可能性を減らすために、回復性の高い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。例として、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。このプロセスは敵対者が通信を傍受できないよう徹底するのに役立ちます。

また、ネットワーク技術は、SIM や GBA [8]や EAP-SIM [9]といった技術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と、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端末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、敵対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。つまり、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なのです。

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構成要素として示したものです。各構成要素はサブ構成要素が

ら構成され、その主要要素だけを取り上げて説明した文書があります。例えば、本文書セットにおいて、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。

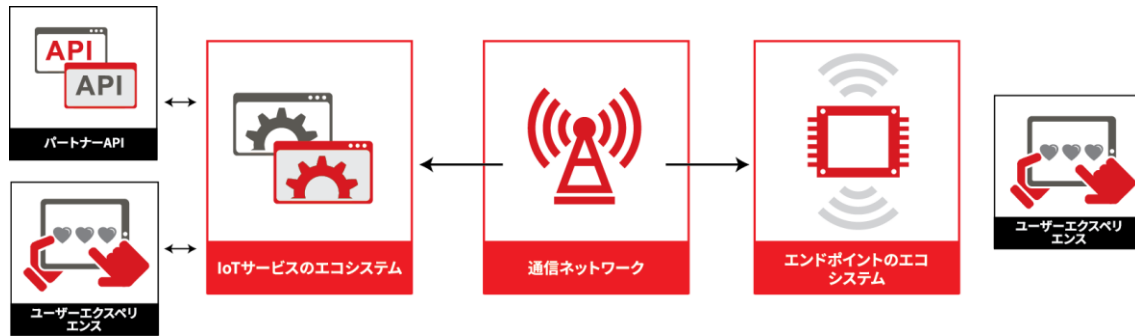


図2:IoTモデルの例示

上の図を見ると、現在あるほぼすべての 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構成要素がわかります。

通信ネットワークは、IoT に固有の構成要素であり、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特別の推奨要件については、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]に記載があります。

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、さまざまな機能を提供し、フィールドで展開するエンドポイントからデータを収集するのに必要とされる一連のサービス、プラットフォーム、プロトコル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、サーバ環境にデータを保存します。このデータは、それに関するエレガントなビジュアル記述を各種ユーザーインターフェースに受け渡すことによって、ユーザーに表示されます。データは、しばしばメトリッ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 を経由して承認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。

本概要説明書で取り上げ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は、CLP.12「IoT サービスのエコシステムのための IoT セキュリティガイドライン」[4]に記載があります。

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、複雑度の低いデバイス、リッチデバイス、ゲートウェイから構成されます。よく見られるエンドポイントの例には、警報装置、デジタル ドアロック、自動車のテレマティクス技術、センサーで動く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。エンドポイント自体がサービスのエコシステムからデータを取得させるリッチ ユーザー インターフェースをエンドポイントに含める場合もあります。

本概要説明書で取り上げ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は、CLP.13「IoT エンドポイントのエコシステムのための IoT セキュリティガイドライン」[13]に記載があります。

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、その適用対象として、多くの企業にとっては情報セキュリティよりも全般的なビジネスリスクのほうがよりなじみがあります。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。

どの組織でも技術リスクを詳細に把握する視点が求められる一方で、次のようなハイレベルの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人のグループ（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。
- どこに脆弱性があるか。

- 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。
- 潜在的な脆弱性を修正または緩和するために何かできるか。
- 新たなまたは拡大するセキュリティのギャップをどのようにモニターできるか。
- 解消できないリスクは何か、それは組織にとって何を意味するか。
- インシデント対処、モニタリング、リスクの改善のための予算はどうするか。

以上の点が、組織の中でエンジニア・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、改善計画と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をも考慮した、より現実に即した視点が得られます。それは、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。組織はそれらのリスクを評価し、許容できるものであるかどうか判断しなくてはなりません。それによって、事業の限界や技術上の制約、特定の脅威への対処を、現実に即して理解できます。

すべてのセキュリティギャップが費用効果の高い方法で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みられる安全性のギャップについて修復・監視・対応するための一連のポリシーや手続き、管理体制を策定（またはアップデート）するものです。リスク評価の結果が、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靱化が図られます。

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（あるいはアップデート）
- 改善策の実行
- 新たなギャップの監視
- 製品またはサービスの向上

これが、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。さらにこのプラットフォームが、組織の全体の役割と責任をコンスタントに評価・改善していくサイクルに組み込まれていく必要があります。

5.2 参照リスクモデル

ここでリスクの評価方法の定義やモデル設計のプロセスの批判をするより、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 の製品またはサービスは、データの作成や収集または共有を目的としたものです。それらのデータの一部は「個人データ」とは考えられず、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。例えば機械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ックスなどがそれにあたります。

しかし多くの IoT サービスは、個人の消費者に関する、もしくは関連したデータを含んでおり、一般的なデータ保護とプライバシー関連法律の適応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ところでは、彼らもテレコミュニケーションに特有のプライバシーとセキュリティに関する規制の適用を受けます。「消費者」にフォーカスした IoT サービスは、詳細な個人データの作成・配布・使用を伴い、個人のプライバシーに影響を与える可能性が大きいものです。例えば個人の健康状態を推測するものや、ショッピングの傾向や買い物場所から個人のプロフィールを導き出すものなどがあげられます。消費者 IoT サービスの人気の高まるにつれて、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ような状況では、この複雑に「結びついた」エコシステムに対し、消費者は以下のような疑問を持つでしょう。

- 個人データを誰が集め、共有し、使用しているのか。
- 具体的にどのようなデータが集められているのか。
- どこから（どのような技術またはインターフェイスで）データが集められるのか。
- いつデータが集められているのか。
- なぜユーザーからデータが集められているのか。
- 個人情報の（安全性だけでなく）プライバシーが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 サービス提供者、またそのデータをキャプチャしたり利用したり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、それらがしばしば矛盾することです。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（静的にも動的にも）把握し、頻繁に向かう先を追跡すれば、ドライバーのライフスタイルや趣味、宗教など、ドライバー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科すことも考えられることから、ドライバー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、その人が住む国以外の法律下に個人データが移動、または存置されます。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考慮されるべき重要な問題です。

もう一つの課題は、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、影響があるとみられる消費者（「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集めてい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、より多くのデバイスがインターネットに繋がれば個人に関するより多くのデータが収集分析され、プライバシーに影響を及ぼすことも十分考えられます。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ィールを提供できます。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、本当の匿名情報のままにしておくことは極めて困難になっています。

健康データなどの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。アメリカでは、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）このような要件からは外れますが、スマートフォンのアプリやクラウドサーバのデータは、個人の特定ができるために規制の対象となるでしょう。（スマートフォンの場合は、ほぼ確実に個人を特定するその他のデータが入っており、クラウドのサーバの場合には、ユーザーを特定できるアカウントに紐付いているからです。）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、人に関する情報や知見がプライバシーに影響を与えうることは認識しています。彼らはリスクに基づいた規制アプローチを重視しはじめ、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注視し始めています。

IoT のエコシステムの信頼性を築くために、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首尾一貫したルールが適用されること保証するべきです。さらに 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、付属資料 A に説明されている手順に従うことが推奨されます。

7 この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のが最も効果的ですが、このガイドは、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対しても役立つものです。読者の製品またはサービスがどのステージに到達しているのかに関わらず、この一連のガイドブックを最大限に活用するために、以下のプロセスをフォローすることが有効です。

- テクニカルモデルを評価する
- 現在のサービスまたは製品のセキュリティモデルを見直す
- 推奨事項を見直し、評価する
- 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

最初の最も大切なステップは、組織が持つ IoT サービスまたは製品の理解です。セキュリティの見直しとリスク評価をおこなうにあたり、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々の構成要素に精通する必要があり、各構成要素がどのようにに関わりあっているのか、またそれらがどのようにそれぞれの環境と関わっているのかを知る必要があります。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。

まずシステムのなかの各構成要素を説明する文書を作成しましょう。その構成要素のソースが何で、どのように使われ、どのような特権レベルが必要で、全体のソリューションにどう組み込まれているのかを確認してください。それぞれの構成要素をサービスエコシステム[3]とエンドポイントエコシステム[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あわせてマッピングします。文書は一般的なクラスにマップすればよいので、それが特定の構成要素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や、コミュニケーションモジュール、またはトラストアンカーなど、前後関係から単純に構成要素のクラスを使用してください。そして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のにどのような構成要素が使用されているか。
- 与えられた構成要素に対し、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。

- そのインプット、アウトプットに既に適用されているセキュリティコントロールは何なのか。
- その構成要素にどの特権レベルが該当するのか。
- 組織内でその構成要素を実装する責任者は誰か。
- 組織内でその構成要素を監視し管理する責任者は誰か。
- 構成要素の中に見つかったリスクを修復するプロセスはどうなっているのか。

これらの質問に答えることにより、技術的な構成要素がお互いにどのように関わりあっているのか、全体の製品またはサービスが各々の構成要素にどのような影響を受けるのかが理解できます。

このプロセスは、CERT/OCTAVE のリスク評価モデル[6]の第1フェーズ、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」ステージにあたります。このテクニカルモデルの評価は、ひとつひとつの重要なビジネス資産のプロファイルの開発や安全性の目的の確立に寄与し、その会社がリスクを評価し、監視し、それに対処するための基礎を築いてくれます。

7.2 現在のセキュリティモデルの見直し

次に、評価の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まで読み進んでください。このセクションを読むと、攻撃者が現状の技術をセキュリティ侵害するために利用するモデルが理解できるでしょう。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終えると、読者は、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。その情報は組織内で共有されるべきで、エンジニアとチームリーダーが共に現在のモデルに対するリスクと脅威を理解することが重要です。

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が必要です。この時点で大まかなアーキテクチャ変更するのは時期尚早です。

このプロセスも、CERT/OCTAVE のモデル[6]の第1フェーズ、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」ステージにあたります。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がどのように決められるかを評価するため、この時点で「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対する知見も示されています。

それぞれの推奨事項に対し、「方法」のセクションがあります。このセクションには、対象となるセキュリティリスクの修復、緩和をサポートする方法の概要が書かれています。高度な見地から書かれていますが、これらの方法は合理的かつ現実的な努力レベルで最大の改善が得られるよう、リスクを全体的な見地から削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」のセクションでは、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的な費用（必要な場合）について説明されています。エンジニアリングタイムや原材料など、ほとんどの費用は明白なもののですが、既に会社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で、必要予算を変更する結果となるような、それほど明白ではない費用も示される可能性があります。特定の費用の額は示されませんが、追加費用を発生させるようなテクノロジーやサービスは特定されます。

特定の推奨事項を実装しなかった場合のセキュリティのギャップを読者が理解できるように、「リスク」のセクションも記載されています。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（もしくは正しく実装しなかった）場合の副作用を、経営幹部が完全に理解しているかどうかを確認すべきでしょう。例えば「データの暗号化」のような推奨事項は自明ですが、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ある種の微妙な脅威は、後々読者にとって想定外の事態となってしまうかも知れません。

また、詳細に見直すための参考文献が示される場合もあります。この文書には全てのテクノロジーやリスク、修復プランについての詳細な情報は記載されていませんが、他の基準や時間を経て実証済みの戦略には、それらが示されています。この一連の文書は、個々の推奨事項のなかで、必要に応じてそのような基準や戦略についての参考資料を提示しています。

「推奨事項」のセクションの見直しの結果は、「セキュリティタスク」のセクションに直結します。この時点では、セキュリティタスクを正しく実装するために、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。そこで、これらのセキュリティタスクが、組織のメンバーに割り当てられている特定の構成要素に結び付けられます。

推奨事項の評価は NIST リスク管理フレームワーク [5] の「アセス」ステップ、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いて、経営幹部はセキュリティ上の脆弱性や価値とリスクについてより深い理解を持っているはずです。経営幹部はここで修正が必要な各々の構成要素についての明確なアーキテクチャモデルを作成します。そして、個々の構成要素とセキュリティタスクに適切な推奨事項とリスクを考慮しながら、その組織によって選ばれたリスク評価プロセスを使用して、個別の構成要素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したところで、セキュリティタスクを充足するために個々の推奨事項の実装に取り掛かることができます。

実装が終了すると、その組織は「推奨事項」のサブセクションと「構成要素」のセクション両面に照らして、リスクを見直す必要があります。組織は、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。これらの文書はこの分野での全ての製品またはサービスをカバーすることはできませんので、その組織で製品またはサービスについて構成要素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かめることが必要なのです。できれば、第三者のコンサルティング会社に、セキュリティについてのベストプラクティスを実装されているかどうかを評価してもらってください。

実装と見直しは NIST リスク管理フレームワーク [5] の「対応」の箇所、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

この時点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。セキュリティは全体のプロセスのエンジニアリングの中で避けられない部分です。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、生き物のように世話をしなければなりません。

要求事項は時と共に変わっていきます。暗号のアルゴリズムは陳腐化したり廃止されたりします。新たなプロトコルや無線技術はその製品またはサービスで同時に使用されなければなりません。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、匿名性、正当性、可用性、信頼性が確実に維持されるよう、常に見直しが必要です。

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

8 実例 – ウェアラブルの心拍数モニター

この事例では、このガイドラインを使って、簡単な心拍数モニター（HRM）の設計を評価してみます。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、一方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観

まずエンドポイントのハードウェアの評価から始めましょう。

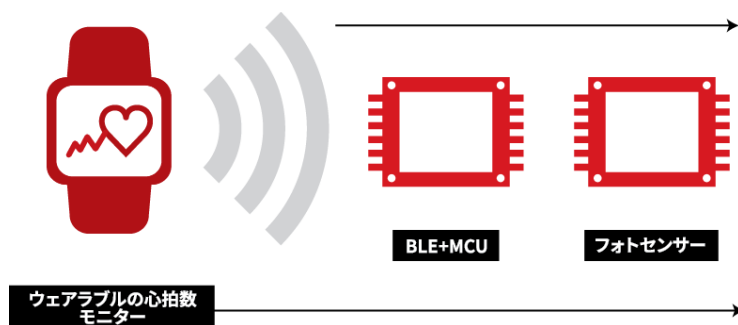


図3- シンプルHRMと主な構成要素

HRM は簡単なワイアレスのウェアラブルデバイスの標準的な構成要素から成り立っています。照度フォトセンサーと Bluetooth 低エネルギー (BLE) トランシーバで稼働するマイクロコントローラです。センサーは脈拍のデータ採取に使用され、マイクロコントローラは、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 トランシーバを経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 Version 4.2 です。

HRM からスマートフォンやタブレットなど他のデバイスにデータを転送するのに、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。このデバイスが作動するのに、これ以外の構成要素は必要ありません。

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 サービス概観

サービスの観点からは、スマートフォンやタブレット上のこのアプリが、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ックスを送信します。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ックスとデバイスの所有者を関連付けさせ、それをそのアプリのサーバのローカルなデータベースに保存するだけです。

データのビジュアル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可能となります。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、エンドポイントで集められたメトリックスを利用してもっと多くの操作をすることもできます。

これはカスタム性もなく不必要に複雑でもない、非常に簡単で一般的なサービスモデルです。

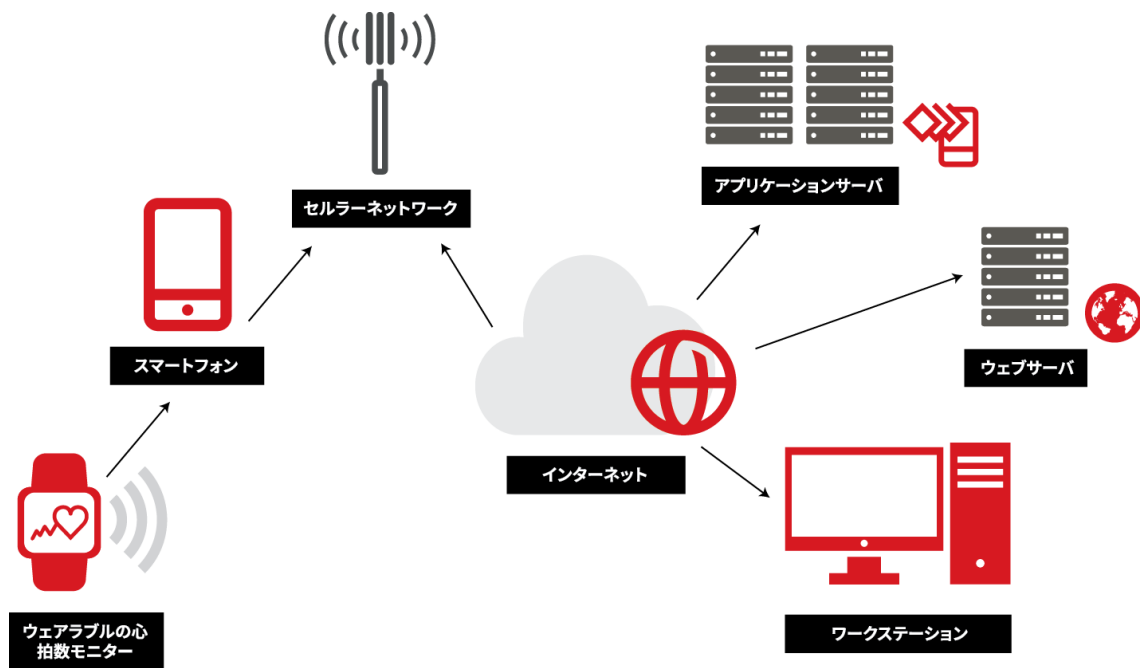


図4- シンプルバックエンドサービスへのデータフロー

8.3 使用例

このテクノロジーを開発した企業は、エンドユーザーが1日を通じて心拍数のデータを取り、それ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考えています。ユーザーが自分の心拍数を長い期間にわたってチェックし、からだ全体の健康を管理してもらうという意図です。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で、自分の健康が改善したり悪化したりするのを確かめることができます。自分のHRMのデータの改善傾向、悪化傾向を確かめながら、ユーザーは自ら目標達成の意欲を高めることができます。

この企業は、医療装置メーカーやヘルスケアサービスの提供者、そのほか心臓発作や脳卒中など多少なりとも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ックスを使用できるパートナーと共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、どの問題が彼らの製品またはサービスに最も関係があるかを確定するのに、エンドポイントとサービスの文書の「よくあるセキュリティに関する質問」セクションを活用しました。

すると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。

。

- 複製
- 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、チームが以下の問題点を特定しました。

- 複製
- サービスのハッキング
- エンドポイントでの異常な作動の特定
- 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「よくあるセキュリティに関する質問」のセクションの推奨に従って、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コミュニケーション両方に最低限のセキュリティを備えていれば済みます。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ので、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の攻撃の恐れはありません。

しかしながらプライバシーの問題は残っており、この企業は少なくとも信頼計算処理ベース（TCB）の個人別 PSK バージョンを使用すべきでしょう。これにより、暗号化トークンは個々のエンドポイントに固有のものとなり、一つのセキュリティ侵害を受けたエンドポイントが全てのエンドポイントにセキュリティ侵害することを防ぐことができます。もし個人用の（固有の）キー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れば、この使用例は複製やなりすましやプライバシー問題の脅威に対して適度に安全だと言えるでしょう。信頼計算処理ベースに関する包括的な説明は、IoT サービス

スの文書[3]とエンドポイントの文書[4]にあります。それぞれのエコシステムのなかでご確認ください。

一方、サーバのインフラストラクチャーには大きな変更が必要です。推奨事項に従って見直すと、エンジニアは大きな不正使用のリスクがあることに気づき、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。
- サービス部門間で責任の分離がない。
- 個人ごとの 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、適切な安全対策が採られていない。
- エンドポイントでの異常な作動を評価するメトリックスがない。

8.5 結果

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

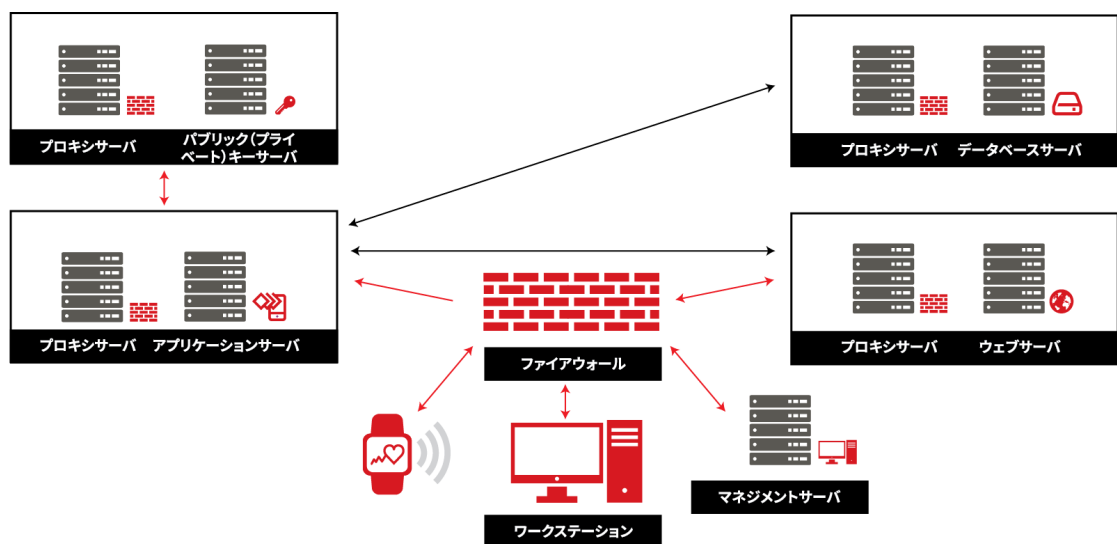


図5- 改善後のサービスエコシステム

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、その技術を簡単に拡大す

ることができます。外部の世界と直接インターフェース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減らす 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、マネジメントのプロダクション環境へ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構成要素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デザイン上の不備を監視するものです。

8.6 要約

全体的に見て、もし現状のままの使用されていれば、このシンプルなテクノロジー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手早くシンプルかつ費用効果の高い変更をいくつか実施すれば、このテクノロジーはアーキテクチャを変えることなく同じフィールドで何年も有効に使用できるでしょう。

サービスエコシステムが拡大していくに従って、ユーザーにとっても企業にとっても脅威はどんどん少なくなっていくます。複製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ています。重要な情報を格納しているシステムは、頻繁に悪用される大衆向けシステムからは隔離・保護されています。モデルは多少複雑にはなったものの、稼働環境全体のリスクは削減されています。

9 実例 — 個人使用のドローン

この事例では、この一連のガイドラインを使って小型の個人用ドローン进行评估してみます。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、一方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観

まずエンドポイントのハードウェアの評価から始めましょう。

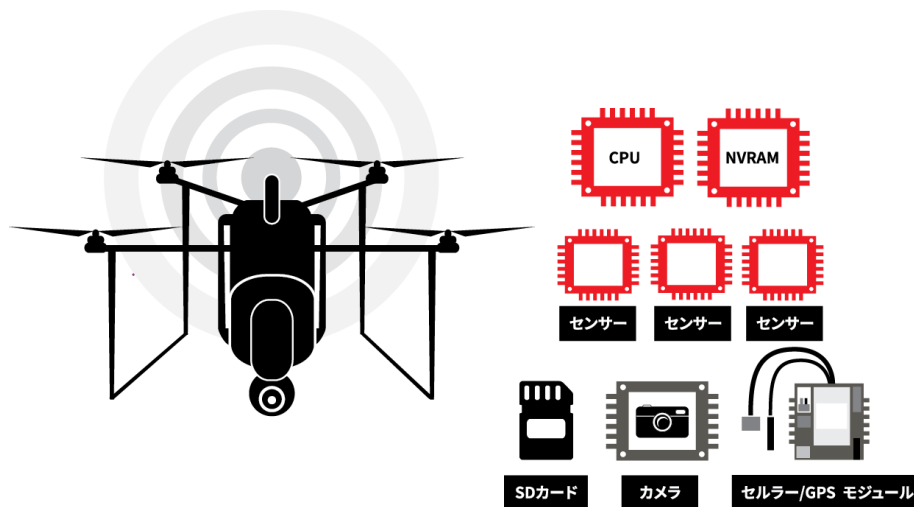


図6- ドローンとその主な構成要素

この個人用ドローンの構成要素は非常にしっかりとしたものです。複数のモーターとセンサー、その他全て並列で効率的に機能するデバイスを備えており、プロセス能力は高度です。このモデルは、ARM Cortex-A8CPU 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。動きやライト、スピード、その他さまざまなものを感知するために、多くの種類のセンサーが必要です。動画やセンサーメトリックス、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いて、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レンジから外れ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われています。GPS は誘導や最低限の自動化のためにも利用されています。

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いますが、他のエンドポイントとのメッセージのやり取りをおこなわないので、ゲートウェイとはみなされません。

9.2 サービスの概観

サービスの観点からみると、バックエンドが使われるのは、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知された場合、操縦者と接続するために限られ

ます。もしドローンが飛行中でセルラーの接続ができるようになっていれば、LTE ネットワークを通じて操縦者が接続してくるのを待とうとするでしょう。しかしもしLTE でコントロールが不能となった場合、最後に飛び上がった場所に自動的に着陸しようとします。

ただしドローンは簡単な自動機能が付いているので、写真を撮ったりビデオを撮影しながら移動するための経路や座標を教えることができます。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、システムにつながっている個々のドローンには、サービスの高い可用性を確保するためにしっかりとしたバックエンドサービスが必要となります。ビデオ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、ウェブのインターフェイスも必要となります。

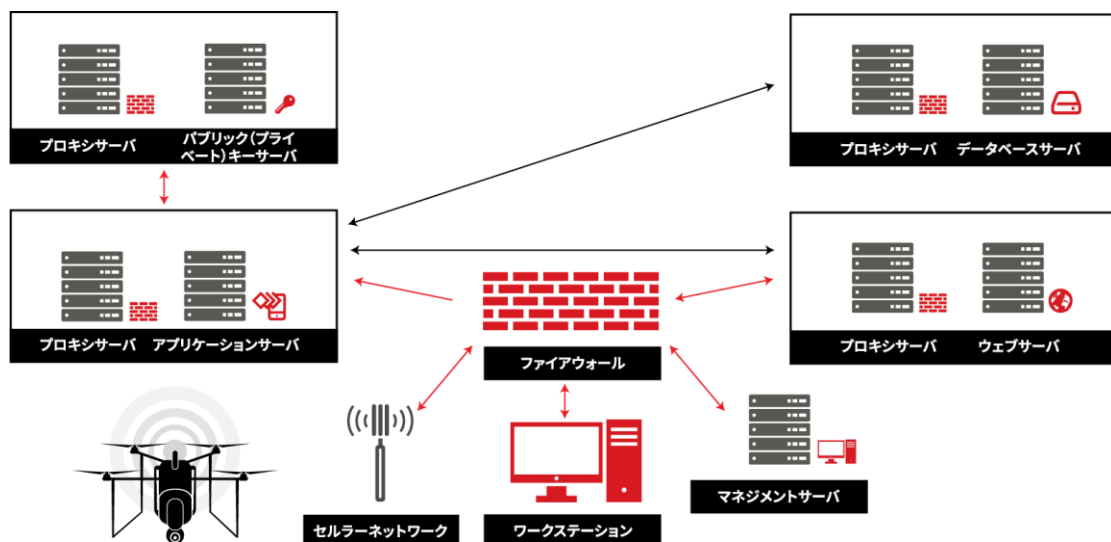


図7- バックエンドサービスへのデータフロー

9.3 使用例

このテクノロジーの開発業者は、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

著しく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シーンの撮影に利用しています。今後は高額映画プロジェクトでも使用されることになり、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、彼らの製品またはサービスに最も関係する問題は何かを確定するため、エンドポイントとサービスの文書の「セキュリティに関してよくある質問」セクションを活用しました。

すると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
- セキュリティ侵害されたエンドポイントの検知
- 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、チーム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「セキュリティに関してよくある質問」のセクションの推奨に従って、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ー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ーは既に大幅に拡張済みだったからです。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

整然として安全なものに設計しておくことが必要でした。しかしながら、企業の予期しなかったニッチな利用方法に関してユーザーのプライバシーが大きな争点となっていたので、企業はさらに研究を進めることに決めました。

一方、エンドポイントのインフラストラクチャーには大きな変更が必要です。推奨事項に従って見直すと、エンジニアは大きな不正使用のリスクがあることに気づき、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無いために、データの流出につながりかねない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ラジオインターフェイス上で正しく認証できない。
- エンジニアはコミュニケーション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

ガイドラインに特定されたリスクに対し適切に対処できるよう、上記の問題に対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きく改善されました。

既存のドローンシステムは既に生産されているので、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植え付けると同時に、ブートローダーも改良することになります。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で偽装しながら、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うま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活

用して、ユーザーごとの個人用キーを作成したからです。こうすることにより、適切なウェブ資格情報を持たないユーザーは、誰も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、実装するには時間がかかりますが、努力を払ってでもやる価値はあるでしょう。

将来のドローンテクノロジーは、内部 CPU のトラストアンカーを実装するかたちとなるでしょう。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、個々のエンドポイントが一つ一つ極めて安全性な状態で増やせるのです。

このような方法で強力な暗号化を展開することは、会社が懸念する他の種類の攻撃をも無効にする可能性もあり、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・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、非認証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。非認証サービスを検知した時に、ドローンが当初の離陸地点に戻ればよいのです。

セキュリティが不完全なドローンを検知すると、内部のアラートで知らてくれるサービスを使うこともできます。それが分かった時点で、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取り扱うかを決めることができます。またこれにより、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、会社はエンドポイントの異常な作動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創り上げるのに明らか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テクノロジーを創りあげるには、非常に多くの作業が必要でした。このシナリオ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、お客様のニーズになん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しかねない不十分なテクノロジーであれば、ここで使わ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 PSKTCB などの信頼計算処理ベース (TCB) のバリエーションについての詳しい情報は、IoT サービスの文書[3]と IoT エンドポイントの文書[4]をご参照ください。

10 実例 – 車両センサーネットワーク

この事例では、この一連の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、一方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観

まずエンドポイントのハードウェアの評価から始めましょう。

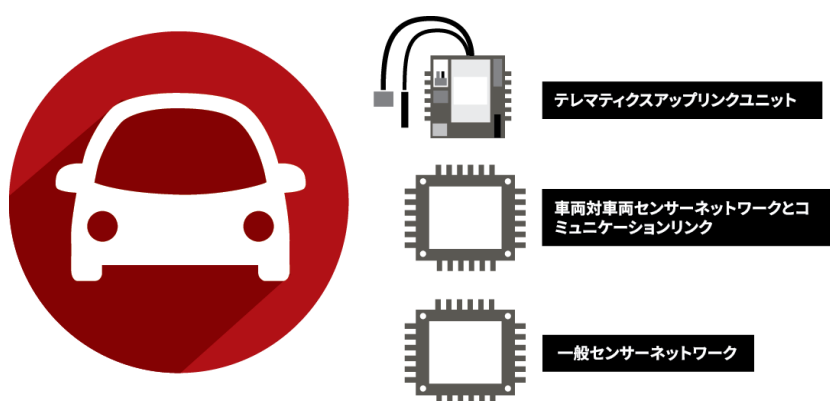


図8- 完全車両センサーネットワークとコミュニケーションシステム

上記のモデルは簡単な図で正確に表すにはあまりにも複雑なものですが、以下の3つのハイレベルの構成要素が含まれています。

- ドライバーの代わりに複雑な意思決定をおこない、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）のイベントを検知し反応する 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ックスを提供する一般センサーネットワーク

近年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コミュニケーションに基づき意思決定をおこないます。このユニットは、消費者であるドライバーと共に、あるいはドライバー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、センサーから集められたメトリックスを基に意思決定をします。構成要素（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しますが、V2V システムも他の車両の存在に反応して意思決定したり、危険な場合に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送る一連の構成要素です。これらのユニットは、危険な場合には正確な意思決定をおこなうよう、一般センサーネットワークから集められた情報を使用します。

エンドポイントエコシステム文書に照らしてみると、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構成要素を備えています。テレマティクスアプリケーション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 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 サービスの概観

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ックスを提供しています。消費者にはこのデータは提供される場合とされない場合があります。このデータはむしろ、その構成要素の潜在的な問題を監視したり特定するために、製造業者が保存することも考えられます。これにより、サービス上の警告が発せられ、事後に消費者に通告されることになるかも知れません。

またこのシステムは、消費者に「リモートアンロックドア」や「スタートエンジン」などの便利なサービスを提供できるように拡大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、離れたところから車両を運転できるようになるかも知れません。

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ッシングユニットでなされますが、ある種の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った機械学習（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。

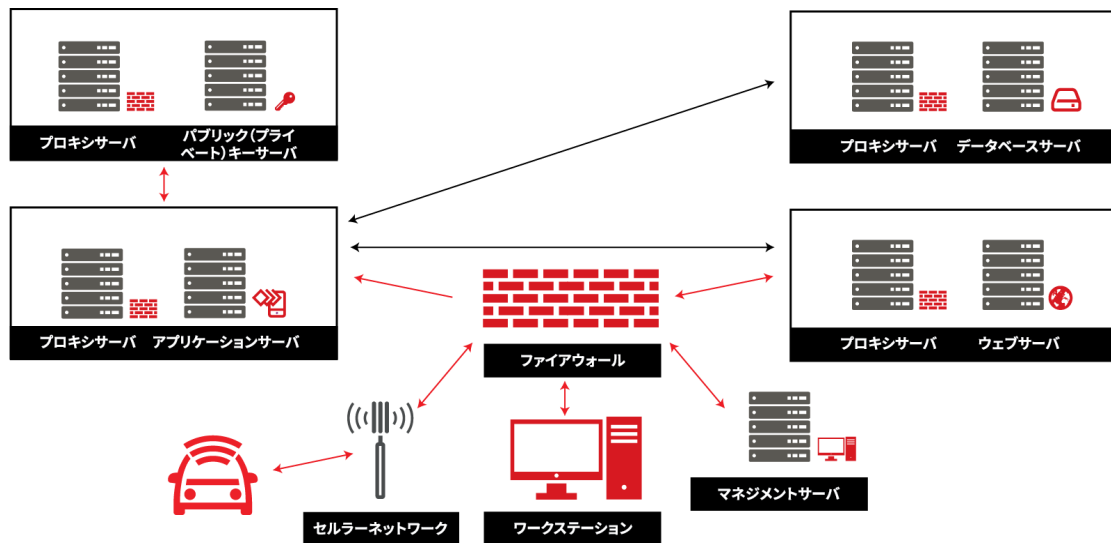


図9- バックエンドサービスへのデータフロー

10.3 使用例

このテクノロジーの使用目的は明かです。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一層スマートな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、極め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、タイヤ破裂のブロードキャスト警告、一時的作動不能オペレーターウォーニングの使用などの危険を伴うシナリオでも、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。

このテクノロジーの興味深い特徴のひとつは、ユーザーにとって完全に透明性が担保されたものになるかもしれないということです。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全くありません。その代わり、センサーのメトリックスを使用して、その時の状況にうまく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作動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、彼ら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「セキュリティに関してよくある質問」セクションを活用しました。

すると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端末によるなりすまし
- サイドチャネル攻撃
- セキュリティ侵害されたエンドポイントの検知
- 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、チーム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作動の特定
- 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、ピア端末による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、コンピューターが正しく認証していないデータにより重要な意思決定をし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極めて瞬時に処理することが要求されるので、理論的にはコミュニケーションに基づく非対称の暗号または PKI を実装することが常にできるとは限らないとされています。しかしこれは正確な言い方ではないかもしれません。むしろ、時間が非常に重要なシナリオでは、的確なセキュリティモデルは事前に準備し、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には、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、危険なシナリオ（例えば自動車同士がぶつかりそうになっているとき）が発生する可能性が検出された時には、安全性が確保されたセッションで瞬時に再ネゴシエートする時間がない時でも、エンドポイントとセンサーの間で確実に安全なコミュニケーションをおこなうことができます。

このように、TCB 実装には拡張が必要ですが、ひとつ興味深いソリューションとしては 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キーを安全に配布することができます。このプロトコルで、多くの危険なシナリオで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、常に環境は信頼の根を植えることはできます。

この環境のなかでもう一つ重要な問題は、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、タイヤ空気圧モニター (TPM) などの簡単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、どのようにしてシステム環境が認識できるのでしょうか。もしセキュリティ侵害されているのを知らずに、コンピューターがタイヤが膨張しているという TPM の情報に基づいて重要な意思決定をした場合、車の安全性の問題が発生します。従って、装置の作動とその信頼性は毎回の立ち上げフェーズで再査定する必要があります。全ての装置はタンパーレジスタンスを備えるべきで、もしセキュリティ侵害があった場合にはネットワークに知らせなければなりません。逆に、センサーネットワークの他の装置が、ネットワーク上でピア端末の信頼性を評価できる方法もあるはずです。

10.5 結果

推奨事項を実装後、車両センサーネットワークは、車両コミュニケーション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した。システム上全てのエンドポイントへのキー配布に GBA が使用され、古いキーが再使用されることが無いよう、毎回立ち上げ毎に新しいキーが配布されています。タンパーレジスタンスを備え、全てのエンドポイントで強力な TCB と信頼された組織的なルートを保ち、リスクが大きく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あとでも、人と車の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ビジネスのリーダーは、会社のリーガルチームや保険会社と協働し、安全性の鍵となるテクノロジーを評価し、利用者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。アーキテクチャの修正をすることで、安全性が鍵となるシナリオでもセキュリティを実装することは可能ですが、何を差し置いても人と車の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。しかしコミュニケーション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

トワークなどの壁で仕切られた環境では、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。人の安全性が最優先されるべき環境では、これは受け入れがたいものです。

付属資料 A IoT サービス提供者向けに推奨されるプライバシーの検証

GSMA では、IoT エコシステムで信頼を築き、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ハイレベル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を GSMA では推奨しています。

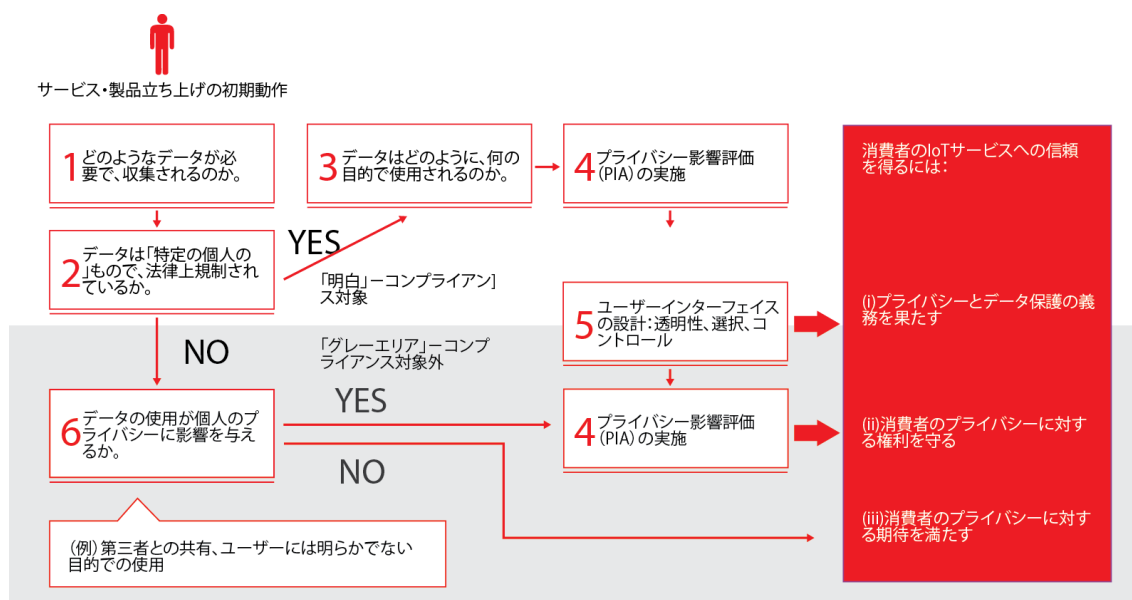


図10- IoTプライバシーデザインのためのGSMAディジションツリー

ステップ	検討事項
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集める必要があるのか。 データに依存するビジネスモデルの最初のステップのひとつは、その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。あるひとつのサービスが必要とするデータは、静的なデータ（例えば消費者の名前や自宅住所）と動的なデータ（リアルタイムでの居場所）に分けられます。例えばもし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提供しようとしているのであれば、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の情報は必ずしも必要ではありません。 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その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か、さらには消費者自身がプライバシー選好をコントロールする選択肢をどのように提供するかを決めなくてはなりません。製品自体に画面が無い場合、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、（例えばモバイルアプリか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。 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。 • 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。 • 集められたデータは「特定の個人の」もので、法律で規制されているか。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。 • プライバシーに関連するライセンスが必要か（例：テレコムのプロバイダなど） • 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、下記のような国や地方、業界固有の法律や規制はないか。 ○ 金融/決済サービス、ヘルスケア業界の規制 ○ 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。 法律上の必要要件を満たす内容を確定した後、その次のステップは、集められ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か、誰とシェアする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。 • データは保存中も転送される時も安全性が確保されているか。 • データフローを明確に設定したか。即ち、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、シェアされるかを特定したか。 • 提供するサービスの流れの中で、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。 • 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（さらにプロダクトデザインはその責任を反映しているか）。 • 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（例えば、アナリティクスの提供者が自分たち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社間の合意に基いたものにするか、そうでなければ、犯した場合の義務と責任を明確に定めた行動規範またはガイドラインを自社で設定し、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 プライバシー影響評価（PIA）の実施とは、 • もし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。 • 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削減する。 • 個人データの取り扱いに関し、より効率的で効果的なプロセスをデザインする。 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。イギリスの Information Commissioner’ s Office（ICO）による出版物[10]や、International Association of Privacy Professionals によるものなど、多くの PIA の実施方法に関するガイドが公表されています。 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。 • そのプロジェクトで、自社もしく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。 • 個人に関する特殊な情報、例えば、健康状態や犯罪歴など、一般的にプライバシー情報だと考えられるものが、プライバシー上の不安または期待を呼び起こすことになるか。 • そのプロジェクトでは、立ち入りすぎ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 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と、リスクを緩和する方法、彼らのプライバシーに関して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と管理できるという確証を与えることで消費者の信用を勝ち得ることです。ここでは下記の質問事項を検討しましょう。 • 消費者がどのようにプライバシーのリスクに気づき、説明された選択肢を選ぶことができるのか。 • 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、契約。 • 移動時と保存中のデータは安全か。 • 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）。 • 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。 ◦ 消費者が、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。 ◦ 消費者が、簡単なステップでプライバシー選好を示すことができるか。例えばウェブベースの「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、モバイルのアプリ、音声コマンドなど。
-------	--

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か あなたが提供する製品やサービスで集めるデータは、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。 • 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導き出すことができる可能性はないでしょうか。その導き出された個人のライフスタイルや習慣や宗教に関する情報は下記に該当するでしょうか。 ◦ 健康保険の契約能力に影響を与えないか。 ◦ 第三者（不動産業者、保険会社など）が、特定の顧客に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。 • もし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、その変更が顧客に与える影響にはどのようなものが考えられるのでしょうか。 ◦ 変更することで、消費者についての新しい情報（例えば位置データ）を収集することになるのか。 ◦ 元々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（例：広告業者）に、既存・新規の消費者データは共有もしくは売却されていないか。 • もし変更する場合、以下の対応をするべきでしょう。 ◦ 変更によって新しい法律が適用される場合のビジネスへの影響をチェックする。 ◦ 消費者告知のプロセスを確立し、必要に応じて本人の同意を得る。 ◦ 消費者にプライバシー選好を変更する手段を与える。 • その他、IoT のサービス提供者には、下記の事柄を推奨しています。 ◦ 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、適切な契約を結んでおくこと。 ◦ もし何か不都合があり消費者がプライバシーの侵害を被った時、消費者への対応窓口の特定も含めて、明確な矯正プロセスを持つておくこと。
---------------	---

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。

付属資料 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って自動車追跡システムを評価しています。このプロセスは、当概要説明書のセクション 6、「このガイドラインの有効な使い方」を捕捉するものです。

B.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、その装置がプロダクト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。そのため、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テクノロジー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します。

• エンドポイントのエコシステム

- 簡単なグラフィック ユーザー インターフェイス (GUI)。これにより、ユーザーは以下のことができます。
 - ユーザーネームとパスワードでログイン
 - 追跡を無効にする
 - 追跡を可能にする
 - 現在の位置を確認しビジュアル化する
- 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
- セキュリティで保護されたプライベート APN
- サービスアクセスポイント
- 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

個別のテクノロジーに関係する情報を確認した後、チームでそれぞれの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、標準的なモバイル稼働 IoT サービスです。

B.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が決まると、その組織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、敵対者がどのようにソリューションに攻撃してくるかを見極めます。

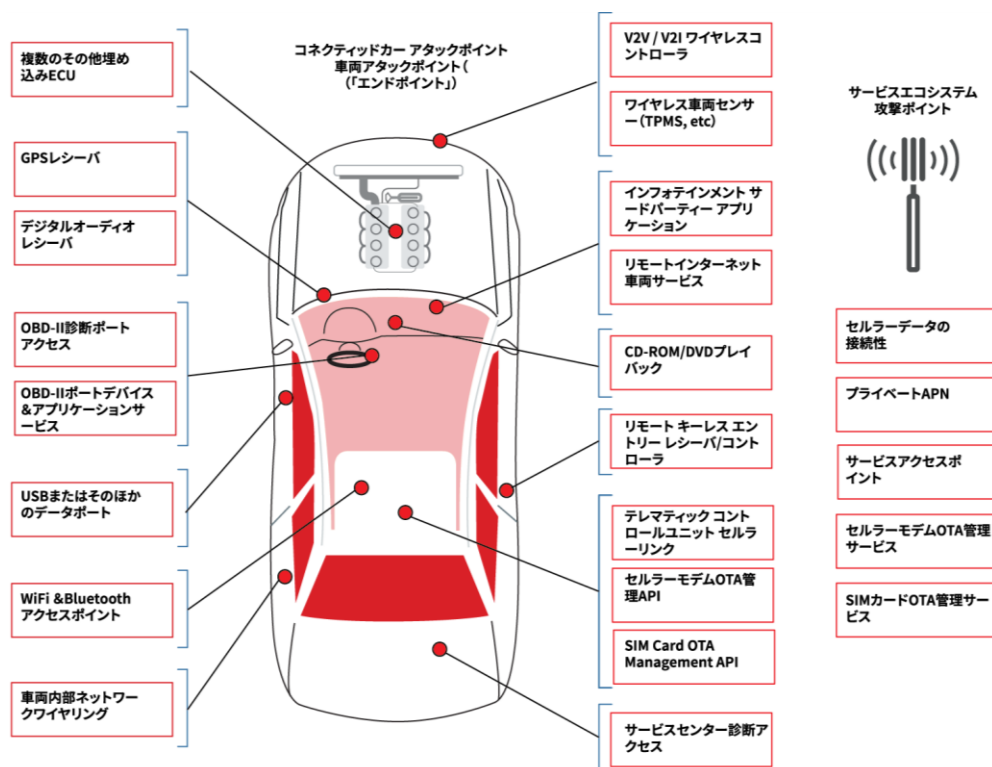


図11- コネクティッドカーの攻撃ポイント

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は無く、モバイルの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し、プライベート APN からコ

コミュニケーション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、または SIM カード OTA 管理サーバ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装置へのセキュリティ侵害ですが、上の図の通り多くのエン트리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べきです。

B.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を終了すると、セキュリティタスクは容易に割り当てることができます。個々のチームは、評価が必要なソリューションの構成要素に対し、特定の人を割り当てる必要があります。ハイレベルの観点（エンドポイント、ネットワーク、そしてサービス）からだけではなく、サブ構成要素のレベルでも評価が必要です。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。

個々の構成要素の担当者が決まると、プロセスを進行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。

- テクノロジーがどのように組み立てられているのか。
- どのテクノロジーがセキュリティに影響を与えるのか。
- そのテクノロジーはどのエンジニアリング関係者が持っているのか。

B.4 推奨事項の見直し

推奨事項の見直しフェーズでは、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。特定の構成要素だけに関連した推奨事項だけに注目するのではなく、それぞれの構成要素が全体の製品やサービスのセキュリティに影響を与えているのかをより適切に掴むために、たとえハイレベルのものだけでも、エンジニアはできるだけ多くの推奨事項を理解する時間を割かなくてはなりません。こうすることで、コスト効率、寿命、管理の観点から最もバランスのとれた修復・緩和措置について、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。

構成要素の担当者は、推奨事項を見直したあと、推奨内容が既に適用されていないかを確認し、推奨をペンディングとするべきかどうかを決めることができます。これにより

、実際に配備する前に、グループで推奨事項の適用性についてあらた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コントロール遂行に悪影響を与える可能性もあるので、作業の進め方としては望ましい方法です。

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。

- 信頼できるアプリケーションベースの使用
- 信頼された組織的なルートの定義
- デバイスパークソナリゼーションの実装
- タンパーレジスタンス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
- エンドポイントのコミュニケーション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装
- デバイス電源アラートの統合

B.5 構成要素のリスクの見直し

次に、各々の構成要素を製品またはサービスに実装したり統合したりする際のさまざまなリスクを特定するために、「構成要素」のセクションに従ってリスクを評価する必要があります。作業を最小限にするために、通常このセクションは、構成要素の担当者だけが見直しますが、チームのメンバーはできるだけ多く読んでおくに越したことはありません。

推奨事項と構成要素のリスクのセクションを見直したのち、以下のようなセキュリティギャップが確認されました。

- 秘密項目は EEPROM 内で保護されずに保存されていた。
- 秘密項目は内部 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。

B.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添って、ソリューションを修正する必要があります。必要に応じて構成要素を再実装し、セキュリティコントロールも追加しなければならないでしょう。

この事例では、チームと協同する GSMA がアプリケーションで作動するトラストアンカーテクノロジーを内包した SIM カードを提供できることがわかったので、既存の SIM カードを利用することで彼らの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、個々の SIM カードは GSMA の標準的なテクノロジーを使って現場でパーソナライズできるので、パーソナリゼーションの問題も解決します。

また SIM テクノロジーは、OTA でコミュニケーションセキュリティを提供することもできるので、プライバシーとコミュニケーション認証実装のニーズも解決してくれます。

SIM の会社固有ゾーンは信頼されたルートを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いながらピア端子の認証ができます。これにより、組織としての信頼に足るルートが構築でき、ピア端子の認証要件の問題を解決してくれます。

製品梱包は、適切なタンパーレジスタンス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、セキュリティキーで暗号化されたデータで書き直されます。

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うよう変更されます。

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、ユーザーによってインプットされたパスワードの安全性の確保を支援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集めるかを確認したりコントロールすることができます。

秘密項目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あらためて評価し直し、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。

B.7 ライフサイクルの継続

承認を受けた構成が出来上がったので、チームはこの段階で技術を配備することができます。しかし、セキュリティの追及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、使用中のテクノロジーが新たに発見されたセキュリティギャップを抱えていないかを確認する方法を、チームで話し合っ

て決めます。さらに個々の事故やギャップをどのように特定し、修復し、回復するのか計画を立てます。そうすることによって、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組織に及ぼすことを防ぐことができるでしょう。

付属資料 C 文書管理

C.1 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 GSMA & Don A. Bailey Lab Mouse Security

C.2 その他の情報

タイプ	説明
文書のオーナー	コネクテッド リビング プログラム
連絡先	Ian Smith - GSMA

私たち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。

連絡先 : prd@gsma.com

ご意見、ご提案、ご質問をお待ちしております。

