cloud security alliance

IoT 早期導入者のための セキュリティガイダンス

2015 年 4 月

日本語バージョン 1.0

日本語版の提供について

本書「**IoT早期導入者のためのセキュリティガイダンス**」は、CSAが公開している「**Security Guidance for Early Adopters of the Internet of Things (IoT)**」の日本語訳です。
本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。
また、この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2016 年 2 月 24 日	日本語バージョン 1.0	

本書は、一般社団法人日本クラウドセキュリティアライアンス　IoT ワーキンググループの以下のメンバーにより作成されました。

二木　真明
新宮　貢
斎藤　知明
勝見　勉
山下　亮一
鶴田　浩司
諸角　昌宏

なお、日本クラウドセキュリティアライアンスについては、以下の URL より参照してください。
https://cloudsecurityalliance.jp

2016 年 2 月 24 日

謝辞

イニシアチブメンバー

Brian Russell, Leidos (Initiative Lead)
Cesare Garlati (Mobile WG co-chair)
David Lingenfelter (Mobile WG co-chair)

K S Abhiraj
Gene Anderson
Megan Bell
Girish Bhat
Kyle Boyce
Poonlarb Chatchawalkhosit (CSA Thailand Chapter)
Michael Cook
Robert de Monts
Tom Donahoe
Chris Drake
Michele Drgon
二木真明
Aaron Guzman
Nader Henein
James Hunter
Gregory Johnson
Alberto Manfredi
Arlene Mordeno
Valmiki Mukherjee
Mats Naslund
Javier Nieto
Chinmoy Rajpal
Tim Owen
Aniket Rastogi
Guido Sanchidrian
笹原英司
Jarrod Stenberg
Shankar Subramaniyan
Thriveni T K
Srinivas Tatipamula
Drew Van Duren
John Yeoh

執筆者

Girish Bhat
Michele Drgon
Larry Hughes
Gregory Johnson
Arlene Mordeno
Jean Pawluk
Brian Russell
Shankar Subramaniyan
Thriveni T K
Srinivas Tatipamula
John Yeoh

目次

概要

この文書は、CSA モバイルワーキンググループ　IoT イニシアチブの成果物である。これは、さまざまな産業を代表する多くのセキュリティとモバイルの専門家からのインプットを使用して作成され、できる限りその分野での既存のガイダンスからの参照と情報を取り入れることで他の業界団体の作業との重複を避け協力関係を維持するようにしている。

この文書のガイダンスは、さまざまな業界を通して利用できるように作成している。これは、複数の業界に渡るアーキテクチャを調査し、各業界をサポートしているセキュリティコントロールを選択することによって行われた。

1. 序論

この文書は、Internet of Things(IoT)をベースにしたシステムを安全に実装するためのガイダンスを提供する。私たちは、IoT の様々な見方を定義するために、ITU-T Y.2060 の用語を使用する。特に、ITU-T Y.2060 は、**IoT** を「情報社会のためのグローバルなインフラにおいて、既存あるいは進化した相互運用が可能な情報と通信技術（物理的、仮想的）に基づいたものを相互接続することによって可能になる高度なサービス」として定義している。 また、ITU-T Y.2060 は以下の定義も提供している:

- **デバイス(Device)**:「通信能力が必須であり、検知、作動、データ取得、データ保存、データ処理の能力を任意に持っている機器。」
- **もの(Things)**: …「物理的な世界（物理的なもの）、あるいは、情報世界（仮想的なもの）のオブジェクトで、通信ネットワークで特定され統合されることができるもの。」

この文書では、IoT の実装者に対して安全な方法で IoT を配備し使用することを支援するためのガイダンスを提供している。伝統的な企業のセキュリティソリューションは、IoT の安全要求を十分には満たしていない。なぜなら、IoT には、以下のような新しい課題がある：

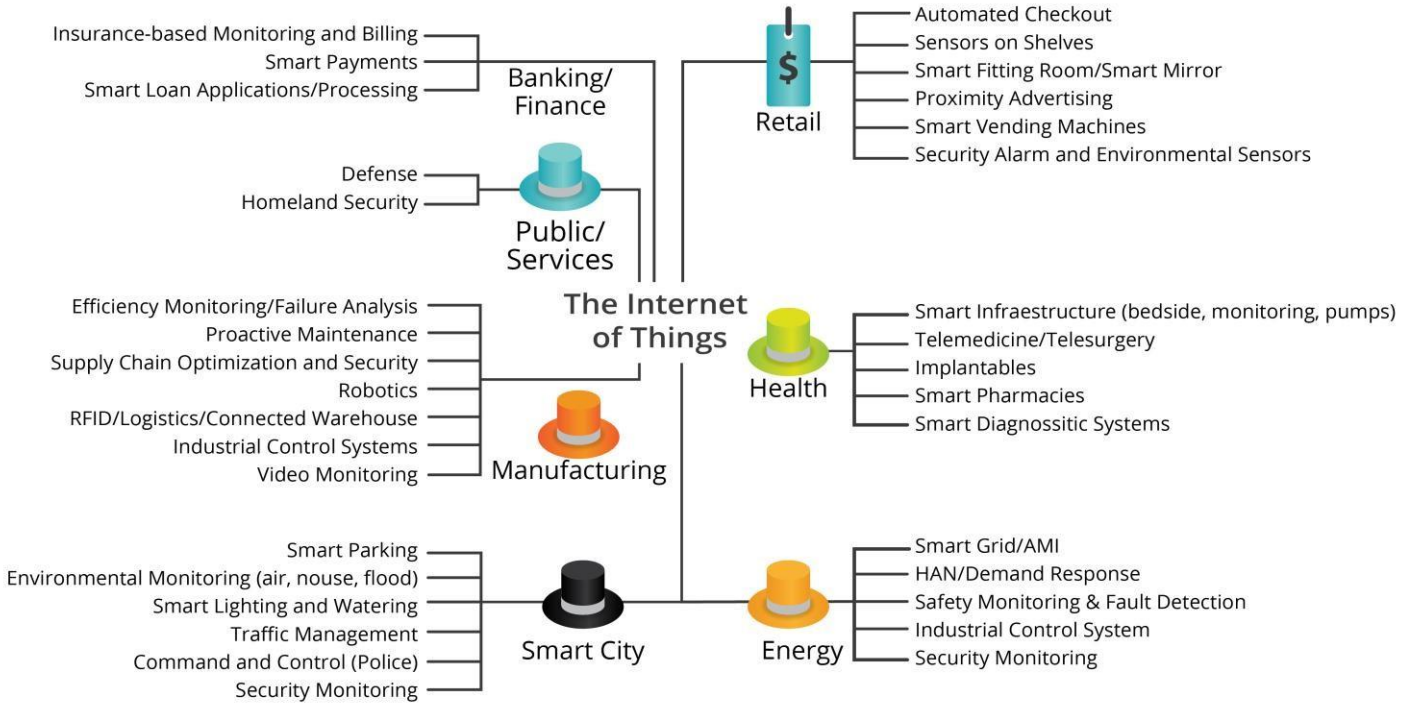
- しばしば混乱を招くプライバシー問題の増加
- 基本的なセキュリティコントロールの課題に取り組まなければならないというプラットホームのセキュリティ上の制限
- 追跡と資産管理に取り組まなければならないというどこからでもアクセスできる移動性
- 更新と保守を日々行わなければならないという課題を引き起こす大規模化
- 境界セキュリティを効率的に行うことを妨げるクラウドベースの運用

2. 目的

市場は、消費者部門(consumer sector)において IoT の広範囲な利用が始まっていることを認識している。ウエアラブル、スマート家電、照明、その他のスマートデバイスが主流になってきている。消費者向けスマートデバイスの人気は、将来に向けて非常に早いペースで成長し続けると予想されている。

ビジネスや公共部門での IoT の採用は、消費者市場に後れを取っている。しかしながら、2015 年のベライゾンの IoT レポート（2015 Verizon IoT Report）は、企業間取引(B2B)における IoT の接続数が 2011 年から 2020 年の間で 28%の年成長率を達成すると予測している。製造、エネルギー、輸送、小売などの産業は、既に IoT を率先して採用している。2015 年の業界における IoT ポジションペーパーで、アクセンチュアは、2030 年までに「業界」における IoT が、米国単独で 7 兆 1000 億ドルの価値があり、効率、安全、生産性、サービスプロビジョニングの拡大をサポートすると予測している。

世界中の自治体もまた IoT を採用し、地理的な領域を超え広がった数千のさまざまなセンサから得られたデータに頼ったスマートシティーになろうとしている。医療セクターにおいても、IoT は、患者の枕元にある機器のようなデバイスに、メーカーがネットワーク接続と知性を組み込んだようなものととらえ始めている。私たちは、人とビジネスの接続の始まりとして IoT の能力をとらえることができる。ここでは、スマートウエアラブルがクラウドを通して情報を集めて、すぐにその情報を医療サービスプロバイダに伝えることができる。輸送セクターは、もう 1 つの面白い領域である。ここでは、乗り物に接続された IoT の概念が出てきており、この乗り物を支えるインフラが勢いを増してきている。さらに、運転手のいらない自動車の実験は、未来をもたらすであろう。ここでは、IoT ベースの路側帯デバイス（RSE）からのセンサーデータを集めて分析する能力がさらに重要になってくる。エネルギー部門では、統合し相互接続されたシステム（例えば、現代の変電所統合システム、スマートグリッドシステム）は、さまざまなユーザにほぼリアルタイムで情報を提供し、運用と性能の効率化にかかわる作業の数を制御するために、電力システムの自動化とリモートアクセシビリティのレベルを増強してきている。



各産業が固有のニーズと要件を満たすために IoT の機能を実装し始めているため、それぞれの固有の実装をセキュリティの弱点の観点から評価すべきであることを理解することは重要である。この文書では、IoT のための一般的な一連のセキュリティコントロールを提供しているが、それぞれ異なった IoT の実装において、ある程度のカスタマイズが必要となる。

いくつかの興味深いサイバーセキュリティのデータが、IoT の大規模採用のためには以下について検討するように指摘している：

- アマゾンの販売上位 25 の SOHO 向け無線ルータモデルの 80%は、セキュリティの脆弱性がある。*[SOHO]
- IT 専門家の 30%と従業員の 46%は、無線ルータの管理者パスワードをデフォルトから変えていない。*[SOHO]
- 幅広く使われているローエンドルータのコードの平均経過年数は、4-5 年である。*[DG]
- Linux.Darlloz という悪意のあるコードに感染したのは、38%はルータ、セットトップボックス、カメラ、プリンタのような IoT デバイスである。*[SYM]

3.個人や組織への IoT 脅威

IoT は組織やシステム全体に設置している新しい機器にもれなく大量に導入されている。データは全ての機器から吸い上げられた上で、解析され、その結果に基づいて何かしらの実行に移る。時には設置された機器自体が何かしらの動作を行うこともある。これを実現するにはセンサーとなる機器がそこら中に張り巡らされ、大量のデータを収集している状態となっている。データ処理によって、もともと見えていなかった繋がりが明らかになり、それにより個人やグループのプライバシーの懸念を引き起こす可能性がある。実質的に様々なプラットフォームに組み込まれている次世代マイクロチップにより、追跡されたり記録されたりしていることに個人が気が付かない可能性がある。全てのケースに言えることは、悪意のある者が IoT の能力を認められていない方法で利用することを防ぐために、全てのコンポーネントにセキュリティを確保することが重要である。

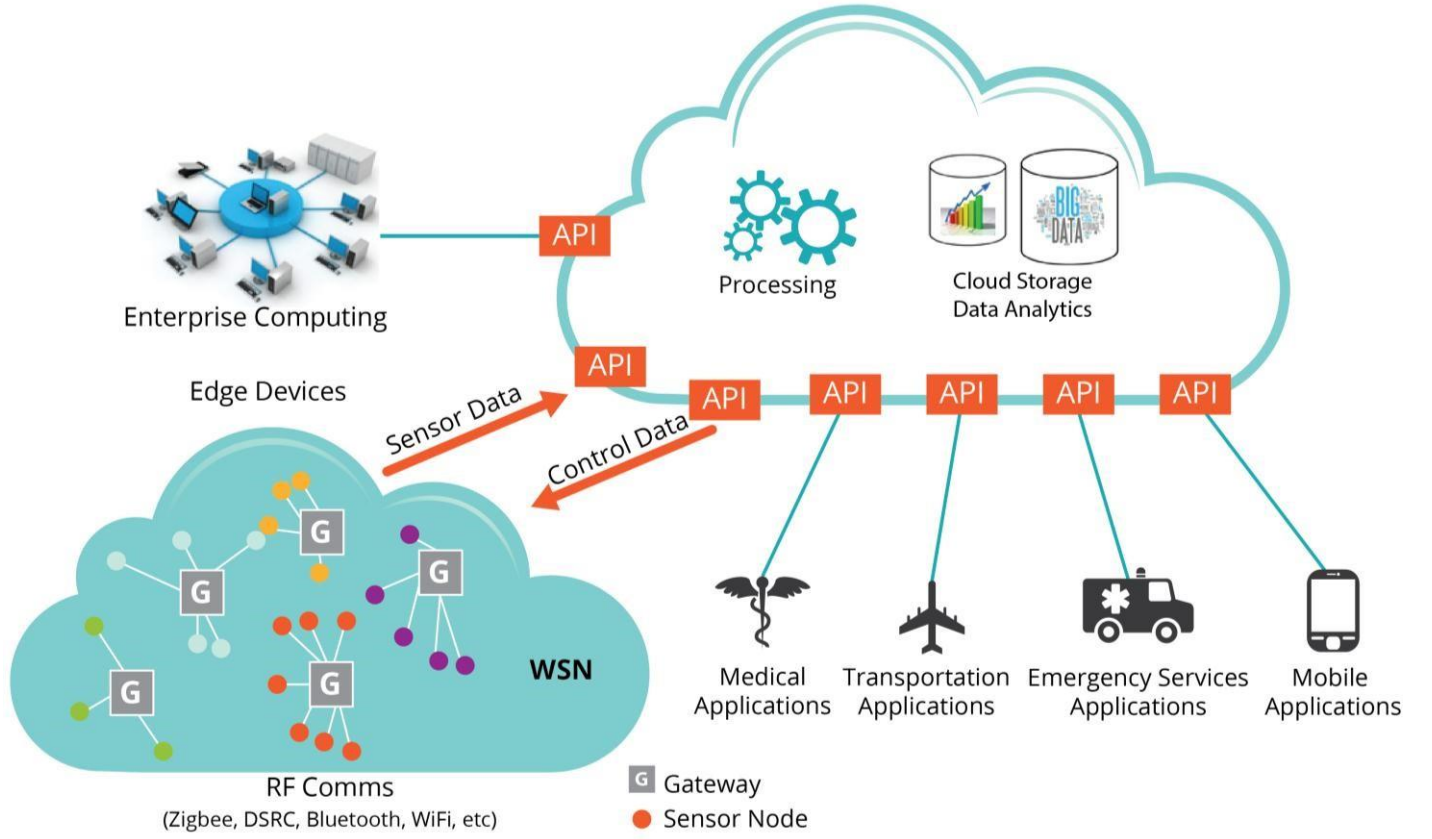
いくつかの事例にある悪意のある者による新しい脅威や攻撃ベクターは、次のような優位性を持っている：

- 許可されていないアクセスを通した物理状態の測定と操作、システムの制御権など(自動車や SCADA、埋め込み型/非埋め込み型医療機器、工場、IoT によりネットワーク越しに操作できる機器を含む)のシステムの制御機能や移動手段、場合によっては人体にとって悪影響や害を及ぼすよう操作する
- 個人の健康情報の改ざんや計測データの操作により、ヘルスケア事業者による正当性のない診察や病気の要因となりうる
- 電子的やリモートコントロールの施錠機器への攻撃を通じて家庭や業務環境への物理的な侵入方法を奪取する
- 車内に設置されたセンサー同士の情報が交換できなくなることにより発生する自動車のコントロール喪失
- IoT センサー情報による DDoS 攻撃により、ガス等のライフラインに発生した安全重要問題の警告が発信不能となる
- 電力系統や温度管理など重大な安全デバイスの乗っ取りによる設備への致命的なダメージの発生
- 個人の健康情報(PHI)も含む機密情報を盗み取る悪意を持った集団による個人情報や金銭の取得
- 多くの異なるシステムやセンサーからデータを集める、または異なる属性や期待値の個人情報を収集して結合することによる個人情報や機密情報の予期せぬ流出の発生
- 金銭の利用時刻や利用間隔の追跡による利用パターンの割り出しから無許可での個人の居場所の収集と記録
- 個人が特定できない状態の収集情報にある位置データから行動パターンを割り出す行為、または分析行為を無許可で行い、人々の活動や振る舞いの収集と記録
- 恒久的に動作する機能を持った小型の IoT 遠隔監視機器の非合法的な監視
- ネットワークや地理的情報や IoT のメタデータを利用して、個人を不適切に分類したりプロファイルしたりすることができる
- 認証されていない POS やモバイル POS を用いて金融のトランザクションを操作する
- プロバイダの提供するサービスの機能不備による金銭的損失
- 離れた場所からハッキングされ、物理的なセキュリティ機能が失われる IoT 機器の窃盗や破壊、機能の妨害
- 組み込み機器(例:自動車、家庭、医療機器)のファームウェアやソフトウェアのアップデートの機能を乗っ取り、IoT エッジデバイスに不正アクセスしてデータを操作すること

- IoT のエッジデバイスを乗っ取り、信頼関係を悪用して会社のネットワークに不正アクセスする権限を得ること
- 大量の IoT エッジデバイスを乗っ取ることによりボットネットを構築すること
- ソフトウエアベースのトラストストアに依存するデバイス内の暗号鍵を入手して、IoT デバイスになりすますこと
- IoT のサプライチェーンにおけるセキュリティ問題を利用して、知られないうちに不正なデバイスを設置すること

IoT はデータ収集や何かしらの動作をするように役目づけられたエッジデバイス群である。これらのエッジデバイス群は独立した機器から構成されている。例えばスマートセンサーやスマートメーター、または電子制御ユニット(ECUs)の付いた通信機能のある自動車などの組み込み型大型機器などである。エッジデバイス群はデータを集め、記録や処理を行う。機器群は直接か、ある種のゲートウェイ機能を持った無線(RF)を用いてつながりあう。これにより最終処理サービスやクラウドサービスと情報交換ができる。データ分析システムはデータを整頓し、場合によっては次の動作をするためのコンポーネントを呼び出す。そして IoT のエッジデバイス群からまとめて得たデータを扱うアプリケーションや、エッジデバイス群から送られてくる情報を分析するアプリケーションに渡す。

The Internet of Things

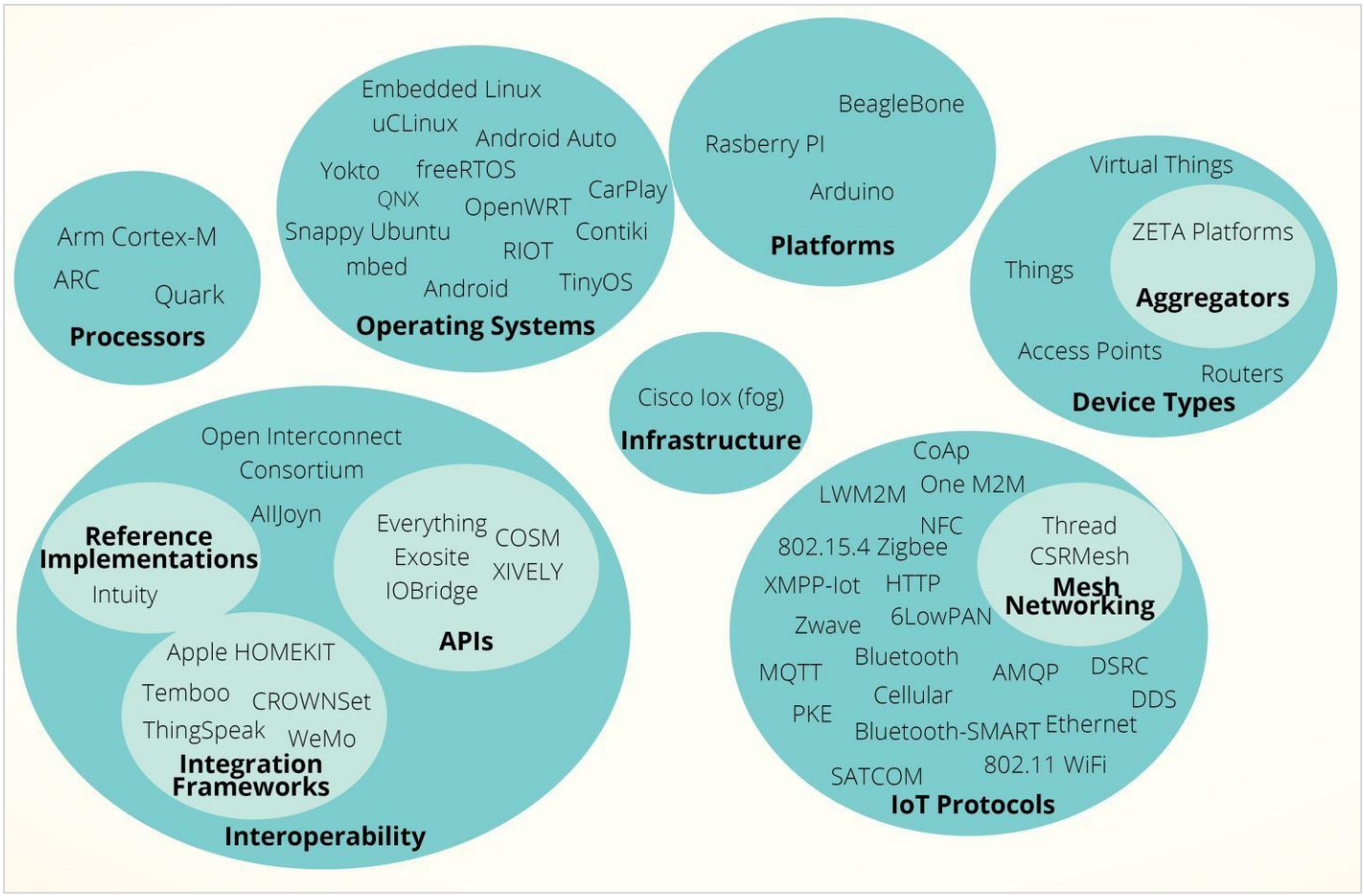


データの生成と分析は IoT に不可欠であるため、そのライフサイクル全体を通してデータ保護することを検討する必要がある。データは、それぞれ異なるポリシーや意図を持った多くの管理された境界を流れるため、このレベルでの情報を管理することは複雑である。個人は企業とは異なったプライバシー目標を確かに持つことになり、そして政府やその他の組織と異なった目標を持つことになる。多くの場合、データは、処理能力が限定的であるため高度な攻撃に対して脆弱なエッジデバイス上で処理されるか保存される。

多くの異なる供給源からのデータが一箇所に集まる場合には、プライバシーに関する潜在的な問題が理解されるようにプライバシーへの配慮が考えられなければならない。プライバシー・コントロールは、IoT エコシステムの様々な箇所で必要とされる。特にデータ取得に対するユーザの同意、IoT パートナー間やデータが保管され、使われるシステムを持った箇所との間のデータの転送が該当する。

IoT エコシステムを構成する様々な技術的、物理的な要素を提示し、IoT を一つの System-of-Systems（統合システム）として検討することは良いことである。組織にビジネス価値を提供するようなシステムの構成は、多くの場合、完全に機能する IoT システムを構成するエッジデバイス、アプリケーション、トランスポート、プロトコル、そして分析機能を含む統合されたソリューションをデザインするためのエンタープライズ・アーキテクチャのように複雑なものとなる。安全な IoT であり続け、IoT の特定のインスタンスが他の企業の IT システムへの攻撃の開始点として使用できない、ということを保証するための取り組みを紹介する。

IoT エコシステム



IDC(International Data Corporation)は、2017 年までに IoT を採用している 90%の企業がバックエンド IT システムの欠陥に苦しむことになるだろう、と考えている。これは興味深いデータで、現在多くの IoT 開発者に採用されるようなセキュリティ工学やセキュアな開発のベストプラクティスの欠如に対する懸念がある。早期に導入している企業においては、安全でない IoT プラットフォームにより脆弱性が露呈しないよう、企業負荷の軽減に努めるべきである。

CSA のガイダンスでは、IoT の導入における課題について論じられており、早期導入者には以下のような目標達成のための提案が纏められている：

- IoT 上で収集されたビジネス、および個人的なデータの機密性と完全性を暗号化提供により保持すること。
- IoT 機能を実装する前に影響調査を行うことにより、プライバシーに関する懸念を理解し、対処する。
- IoT のデバイスライフサイクルコントロールと、レイヤード・セキュリティ・アプローチにより、IoT をターゲットとし、組織の資産を狙う攻撃からインフラを保護する。

- セキュリティの脅威と戦うために、セキュリティ・ベンダー、業界団体、CSA と情報を共有し、包括的なアプローチを行う

4.安全な IoT 配備への課題

安全な IoT 実装を配備するための課題は多々あり、マーケットに存在する数々のセキュリティ技術が企業の IoT リスクを和らげるだろう。しかし IoT もセキュリティ工学に対する新しい課題を産み出し続けている。これらの多くは解決のための最適かつ長期的なアプローチを決めるために、突っ込んだリサーチや業界を越えた協力が重要となる。この表は文書の後半で詳述する CSA が推奨する IoT セキュリティコントロールの対応付けと IoT アーリーアダプターが直面する最大級の課題に対する CSA の見解である。

鍵となる課題	課題の論点	CSA　IoT セキュリティコントロールとの対応付け
多くの IoT システムは設計や実装が貧弱で、様々なプロトコルや技術を使っているため、構成が複雑化している。	IoT には、エッジ（末端の）デバイス、メッセージ&トランスポートプロトコル、アプリケーションプログラミングインターフェース（APIs）、データ分析、ストレージ、ソフトウェア、そして様々な他の技術概念が包含される。エッジデバイスはそれ自身複雑で複数の技術レイヤから成り、ハードウェア、ファームウェア、ソフトウェア、そして多くのプロトコルの理解が要求される。これらのすべては多くの産業にまたがった無数の利用事例に対して適用できる。 システムの安全を確保する前に、システムを安全にするための機能的技術的詳細を最初に理解することが重要だ。設計プロセスの初期段階でセキュリティ要求を組み込むために IoT 機能の開発者とセキュリティエンジニアが協業することが必要になる。企業の IoT は系統的なシステムセキュリティ工学アプローチで実装することが望ましい。 システムセキュリティ工学アプローチを IoT 実装に取り入れることで、設計者は単純化が可能な複雑な領域を特定出来る。例えば、使用するプロトコルと接続点を最小限にした実装などが挙げられる。	#2: 新しい IoT システムを建築し配備するために安全なシステム工学アプローチを適用

鍵となる課題	課題の論点	CSA IoT セキュリティコントロールとの対応付け
成熟した IoT 技術やビジネスプロセスの欠如	IoT をサポートする標準はまだ十分に開発されておらず、プラットフォーム、プロトコル、インターフェイスは競争に晒されている。標準の欠如は複雑性を増加させ、脆弱性を生み出し、攻撃者に企業への侵入機会を与える。	#2: 新しい IoT システムを建築し配備するために安全なシステム工学アプローチを適用
ライフサイクル保守と IoT デバイスの管理に必要なガイダンスの不足	多くの IoT エッジデバイスの基礎となる限られた能力しか持たないオペレーティングシステムに関する安全な構成のガイダンスは限られているかもしくは存在しない。 IoT デバイスでのファームウェア、ソフトウェア、およびパッチ更新の実行には、特定の更新をプロビジョニングするという義務と責任をサプライチェーン全体にわたって考慮した新しいアプローチが必要だろう。 組織が IoT 資産を調達する際も、そのライフサイクルを通じてパッチやソフトウェア更新を受け取り続けることがベンダのライセンスモデル上で保証されていることを理解し、同意しなければならない。もし IoT デバイスに必須のセキュリティ更新が遅れた場合、攻撃者はより簡単にそれらを搾取するだろう。この点について、IoT デバイスが各ベンダから最終的にはサポートされなくなることを組織は考慮しなければならない。 IoT デバイスの稼働状況や、それぞれのデバイスのソフトウェアやファームウェアの状態を掌握することも課題である。IoT デバイスの数は、それ自体が効率的管理という面での課題をもたらすことになる。	#5: IoT デバイスに対するライフサイクルコントロールの定義

鍵となる課題	課題の論点	CSA　IoT セキュリティコントロールとの対応付け
IoT 固有の物理セキュリティ懸念	多くの IoT エッジデバイスは、一般に公開された環境で配備されるため、攻撃者はより簡単にこれらを入手して解析することができる。多くの IoT エッジデバイスの性能に限界があり、暗号鍵のような機微なものを保護するために（容易に解析できる）ソフトウエアベースのソリューションを使用せざるを得ない点が懸念される。 十分なリソースを持つ攻撃者はこれらのエッジデバイスをリバースエンジニアリングできる。理想的には耐タンパ性が実装されるべきだが、常に実現できるとは限らない。多くの IoT アプリケーションデバイスが低コストを求められているため、攻撃と改ざんに耐えるデバイス能力と相反するからである。	#3: IoT 資産を守るレイヤーセキュリティ保護の実装
IoT プライバシーの懸念は複雑で必ずしも明白ではない	いくつかのプライバシー懸念は特定が難しく、いくつかの懸念はトランザクションに対する識別情報や位置情報といったものの保護を実施するだけでは解決できない。	#1: ステークホルダーのプライバシー影響分析と、IoT 開発と展開に対するプライバシーバイデザインアプローチの採用
IoT 開発者が利用できるベストプラクティスが少ない	多くの IoT 開発者は安全な開発のベストプラクティスに精通していない。新しい IoT ベースの機能を作り出そうと焦ると新機能のセキュリティは疎かになりがちである。	#2: 新しい IoT システムを建築し配備するために安全なシステム工学アプローチを適用

鍵となる課題	課題の論点	CSA　IoT セキュリティコントロールとの対応付け
IoT エッジデバイスの認証認可標準の欠如	低電力でウェアラブルなデバイスの要求は、実装が成熟しておらず、安全な暗号化や認証もない単純な無線プロトコルを流行らせた。これらのプロトコルは短時間で攻撃でき、また攻撃に際して物理的接触が不要だ。 いくつかの IoT デバイスは認証機能がない。また、その他のものも（機能は）限定的だ。多要素認証をサポートするものは極めて少ない。一般的に IoT エッジデバイスで多要素認証をどうやって使用するかは明らかではない。伝統的な二要素認証の主要な利点のひとつは、”要素”の一つがもうひとつの要素とは別の方法で与えられることにある。しかし、IoT デバイスにおいて、両方の認証要素（例えば鍵）が同じデバイス上に保管されている必要があり、要素を分離して管理するという利点が失われる。 いくつかの標準や商用オプション、例えば証明書認証、Google のような商用あるいは半商用のアイデンティティプロバイダが利用可能ではあるが、それらはデバイス固有の（認証）プロファイル[1]や認可オプションを作る機能が欠如しており、また、それらのサービスプロバイダを使うためのプラバシー要件も検討され尽くしてはいない。	#6: 組織の IoT 開発のための認証/認可フレームワークの定義と実装
IoT ベースのインシデントレスポンス活動に対するベストプラクティスが無い	組織は IoT デバイス、鍵、および証明書などへの侵害が発生した際の対応を計画できなければならない。これには侵害されたシステムとデバイスのフォレンジック分析の実行を含む。	#5: IoT デバイスに対するライフサイクルコントロールの定義

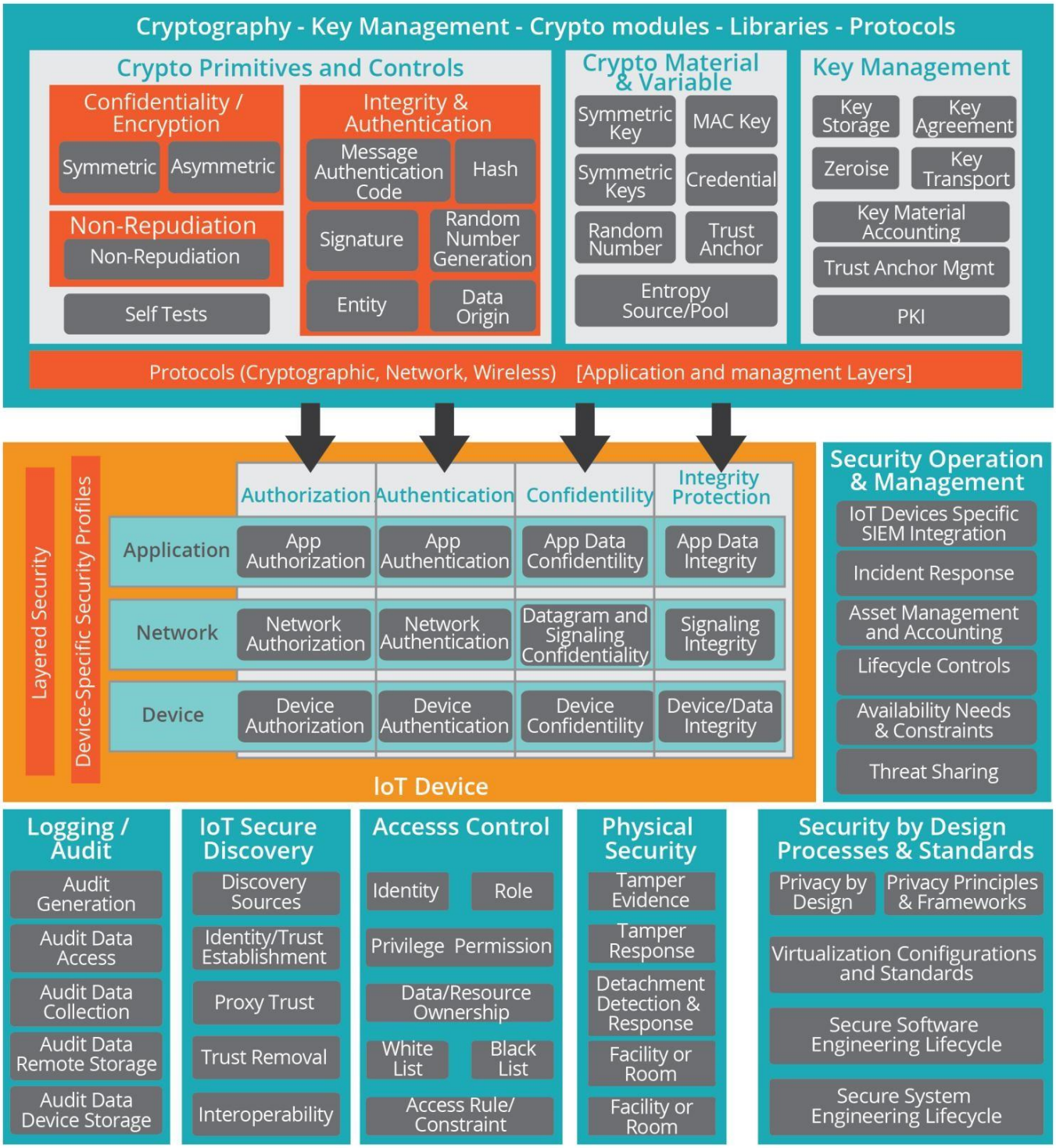
[1] こうしたサービスは人による対話型の認証のみを実装していて、デバイスによる認証で利用するのは困難であることが多い

鍵となる課題	課題の論点	CSA　IoT セキュリティコントロールとの対応付け
IoT コンポーネントに対する監査およびロギング標準が定義されていない	セキュリティイベントに対する IoT エッジデバイスのモニタリングには独特の困難がある。これらエッジデバイスの多くは単一目的のセンサーで、すべての操作をトラッキングする能力が無い。他のデバイスはバッテリーの制約で監査ログ送信用の RF 接続を維持することが難しいかもしれない。IoT デバイスのセキュリティ状況をほぼリアルタイムに手に入れることは難しい。 その他の課題として、広範囲に分散した IoT セグメントから単一のイベント管理システムへのログデータの集約及び、実際にこれらのセグメントのアクティビティからインテリジェンスを引き出すことなどが挙げられる	# 7 : 組織の IoT エコシステムのためのロギング/監査フレームワークの定義と実装
セキュリティデバイスやアプリケーションと IoT デバイスが連携するためのインターフェイスが限られている。組織の IoT 資産に対するセキュリティ状況の認知（監視）を行うための方法論を確立するという視点がまだない。	組織に存在するセキュリティシステムに IoT デバイスを統合することで、組織のセキュリティ状況を認識できるようになる。不幸にも現存する SIEM システムと接続可能なインターフェイスは無く、ID 認証管理システムや他のセキュリティシステムとの接続についての選択肢も限定的だ。これが実情であるとすると、IoT デバイスプールと組織のセキュリティ基盤の間をとりもつような機能をサポートする中継製品が提供されるようになるだろう。	#3: IoT 資産を守るレイヤーセキュリティ保護の実装 #6: 組織の IoT 開発のための認証/認可フレームワークの定義と実装 # 7 : 組織の IoT エコシステムのためのロギング/監査フレームワークの定義と実装

鍵となる課題	課題の論点	CSA IoT セキュリティコントロールとの対応付け
マルチテナントをサポートする仮想化 IoT プラットフォームを実現するためのプラットフォーム構成に対するセキュリティ標準が未成熟	この考え方は、クラウドをデバイスにアクセスするための全機能をサポートするように拡張したような環境での利用を想定している。（たとえば、二つの異なる企業が、クラウドにホスティングされ、同一の物理的な IoT プラットフォームを共用してビジネスを行うような場合である） その結果、軽量だが安全な仮想化/（テナント間の）分離のためのソリューションが必要になる。	#3: IoT 資産を守るレイヤーセキュリティ保護の実装

5. 推奨セキュリティ管理策

IoT の機能を導入しようとする組織に、以下の管理策を推奨する。これらの管理策は IoT に固有の特性に合わせたものであり、IoT の初期の活用主体に、この新しい技術につきもののリスクの多くを緩和するものである。



管理策	実施事項
1	関係先に対するプライバシーインパクトを分析し、IoT の開発と配備に際して、プライバシーバイデザインのアプローチを用いること
2	新しい IoT システムの構築と配備には、セキュアなステムエンジニアリングのアプローチを用いること
3	IoT 資産の防衛のために階層化セキュリティ保護を実装すること
4	機微な情報の保護のために、データ保護のベストプラクティスを実装すること
5	IoT デバイスのライフサイクル管理策を設定すること
6	組織における IoT の配備のために認証・認可のフレームワークを設定し実装すること
7	組織における IoT エコシステムのためにログ管理と監査のフレームワークを設定し実装すること

5.1.関係先に対するプライバシーインパクトを分析し、IoT の開発と配備に際して、プライバシーバイデザインのアプローチを用いること

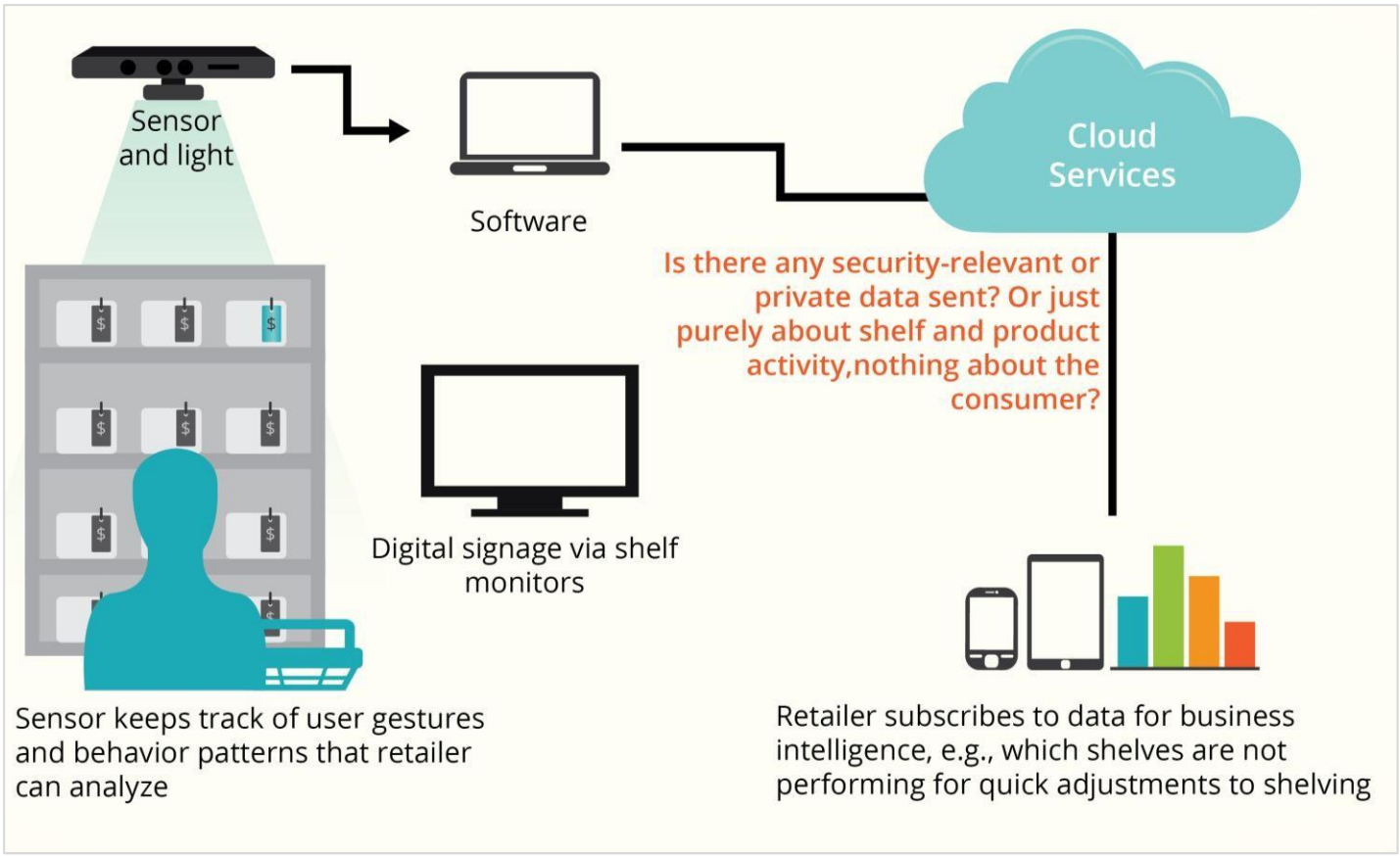
IoT は組織にデータの収集と分析のたのめ強力なツールを提供する。このデータは様々な形態で提供されるが、IoT の場合、多くは内在のデータであり、注意深く解析することにより収集または集約することができるものである。組織が IoT の実践を始める時、センサー、ビデオカメラその他の情報収集用ハードウェアの設置が行われる。これらの IoT コンポーネントは誤って公共の場所や個人の宅内に置かれることがあり、場合によっては個人の利用も起こる。IoT コンポーネントの多くは GPS トラッカーを備え、個人や個人の資産（例：車、電話）の存在場所の追跡が可能である。IoT の別の側面は、多くの IoT システムの間で収集するデータの種類に重畳が起こることである。従い、例え二つの収集システムが完全に別の主体によって運用されたとしても、データの集積により機微な情報が露わになる潜在的可能性が生じる。このような場合、企業のマーケティング担当や悪意をもった攻撃者は、対象の個人に追跡について悟られない状態で、この集積されたデータをその目的のために利用できる。

IoT におけるプライバシーに関する特徴的な課題の一つは、データ収集デバイスやセンサーが、社会を圧倒する能力をすぐに持つようになることである。これらのデバイスは場合によっては悪意をもって利用され、ある場合には個人から追跡について同意を得ていない情報を意図しないうちに入手してしまう。システムの管理者の立場からは、個人から収集された意図しないデータに対してどんな行為が許されるのか、という点であろう。

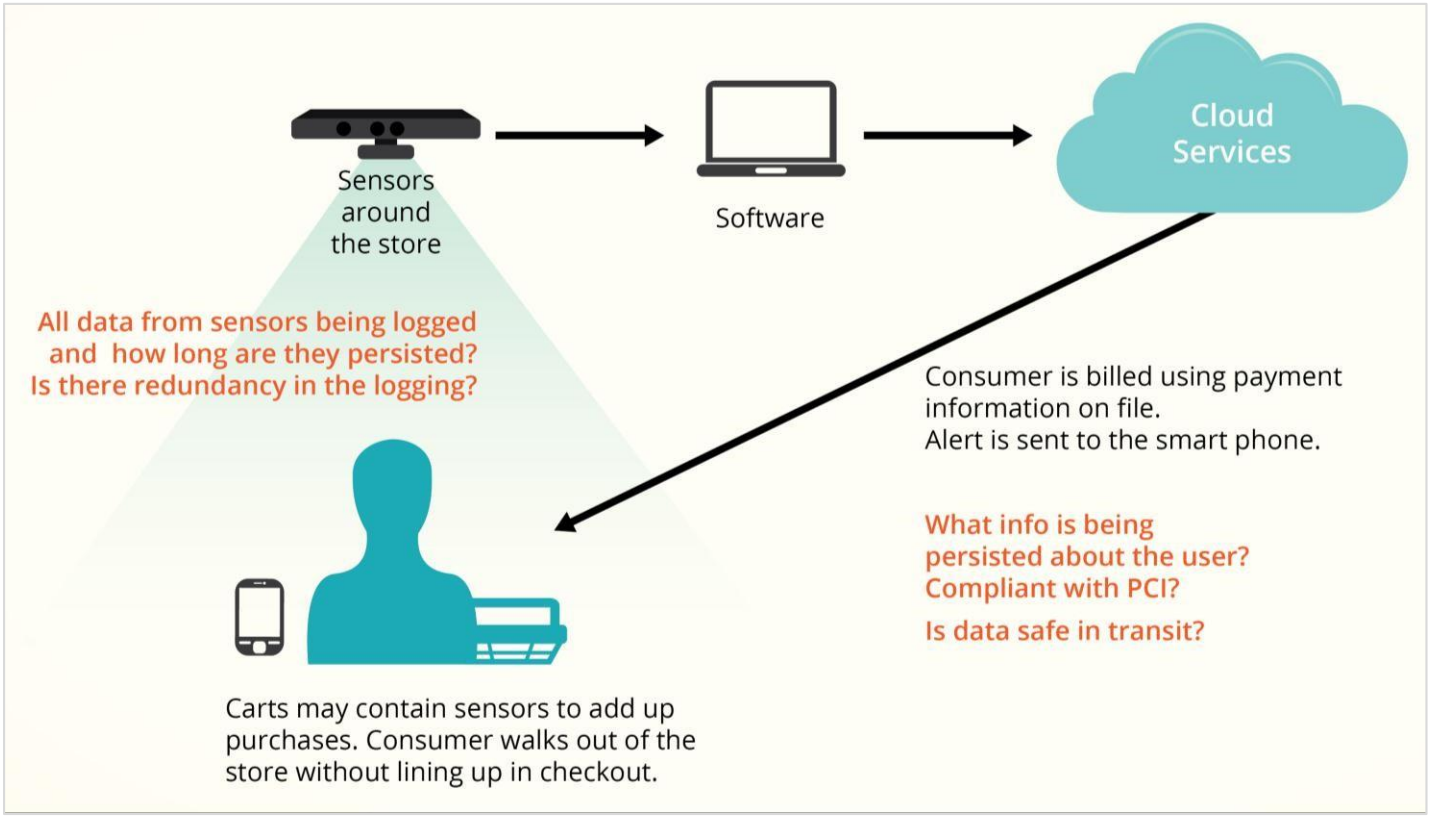
IoT センサーはまた一方で、個人の知覚を高めるように使うこともできる。そのような場合、対象の個人は何らかの IoT システムと相互作用していることを知らされることになる。その典型的な事例は小売業に見られる。小売業における IoT の配備の事例のいくつかを以下に示す。これらの事例は、関係者のプライバシーに対して常に配慮することを確実にするために、IoT システムの設計に際して確認すべき点を理解するのに、よいベースを提供してくれる。

以下に示す図からわかるように、多くのデータは消費者個人に寄り添うような IoT システムによって収集される傾向にある。

棚に設置されたセンサー

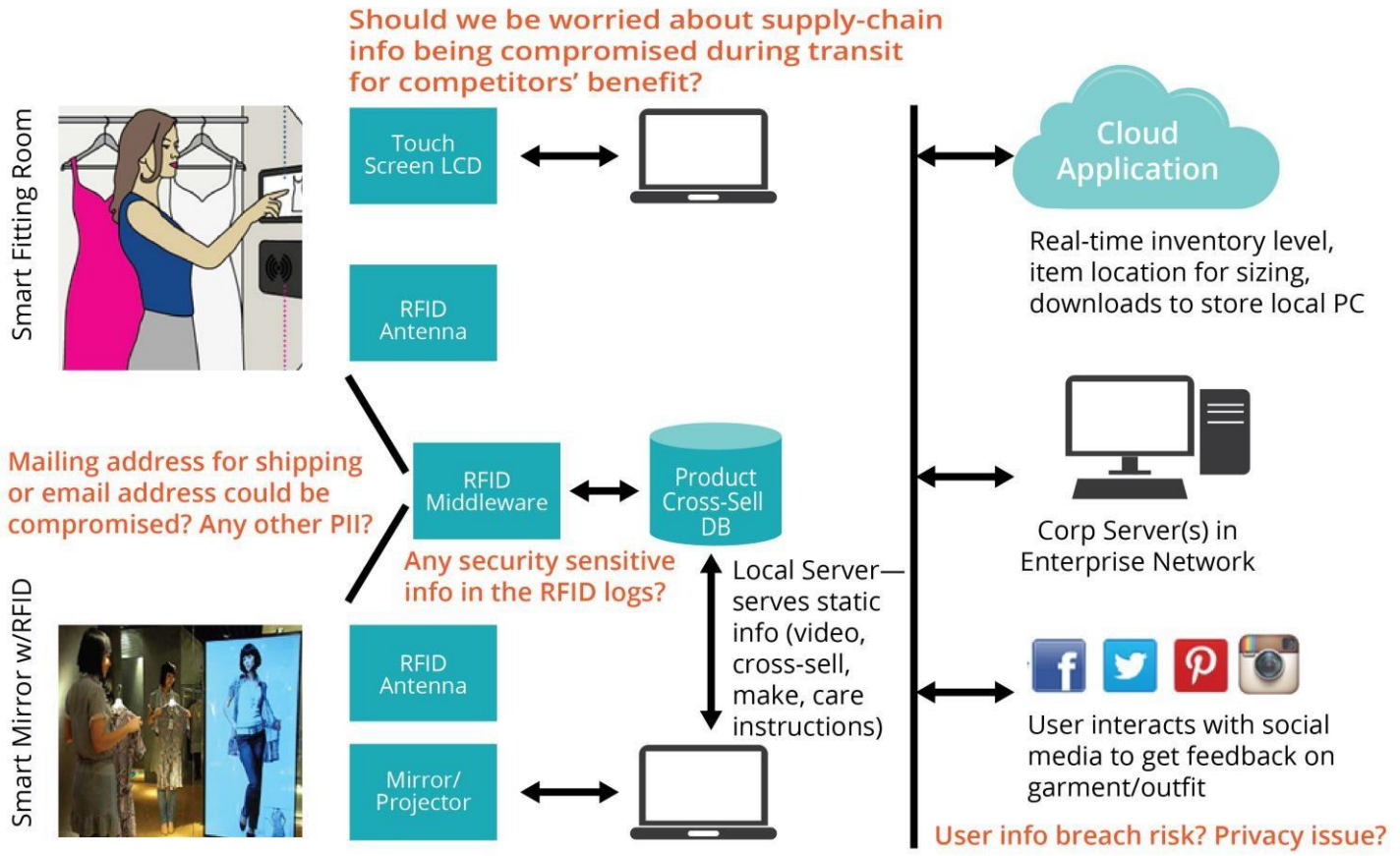


自動会計システム



各ユーザについてどんなデータが把握されるのかに対して厳密に配慮を行い、法令遵守とプライバシー保護規制とってどんなインパクトをもたらすか、考慮する必要がある。同じことは、業界標準への準拠についても言える。例えば PCI は、個人特定情報の保存および送信に際しての暗号化を義務付けている。

スマート試着室／スマート鏡



全ての機微な情報が適正に保護されていることを確認することに加え、サプライチェーンに関連するリスクについても配慮することが重要である。IoT システムを構成するコンポーネントがサプライチェーンの中で侵されていたとすれば、機微な情報が暴露されるリスクは高まる。

近接型広告

もう一つの考慮要素は誰が保存されたプライバシーデータにアクセスできるのかということである。データは第三者に提供される可能性がある。すべての機微な情報に対するアクセスは監査目的のために記録され、規則への準拠性についてチェックされなければならない。

IoT におけるプライバシー問題の複雑性の観点から、IoT に基づく機能を提供する全ての組織にとって重要なのは、関係者の機微情報の保護を確実にするために必要な資源を投入することである。IoT を構成する場合、以下のプライバシーバイデザインの基本原則がシステムに適切なプライバシー保護を組み込むのに役立つ。これらの基本原則はいかなる組織においても、IoT システムを構成する種々のコンポーネントの実装を設計する際に参照するとよい。欧州連合(EU)の第 29 条データ保護作業部会は 2014 年 9 月にガイダンスを発表し、すべての IoT 関係者は、これらの基本原則を、世界のどの地域における実装に際しても適用するべきであるとしている。以下の各節は、これらの基本原則について、IoT の実装に際してそのプライバシープログラムの遵守を組織が行うのに際して活用できる。

5.1.1.プライバシーバイデザインの原則

IoT システムの利用者はそのシステムからの、または利用者に関する全てのデータについて周知され、データ収集の仕組みからのオプトアウトを細かいレベルでできる機会を提供されるべきである。IoT デバイスの多くが適切なユーザインターフェイスを備えていない場合があることに対する心配を踏まえて、組織は利用者にお知らせし選択肢を提供するための適切な方法を用意すべきである。

5.1.1.1. 受動型でなく能動型、事後緩和型でなく未然防止型を

IoT システムの構造においては、システムを稼働状態にする前に全ての関係者に至るプライバシーの波及に関する可能性について配慮することが重要である。最初に、データのタイプ（類型）に着目し、各データタイプについて何が機微であり、どの規制が適用されるのかを分析する。次に、より深い分析を行い、種々の IoT コンポーネントの運用における間接的なプライバシーへの波及について理解する。例えば、接続先の車を追跡するアプリケーションの場合、その追跡が、他のシステムが収集したデータと結びついた時に、例え匿名化していても、特定の個人やグループに結びつく運転パターンを明らかにする可能性があるかを確認することが重要であろう。他の事例として分析用に電力会社に提供されるスマートメーターのデータが挙げられる。もしそのデータに対するアクセスが厳密に管理されていない場合、攻撃者は在宅情報を入手することができ、物理的な攻撃の可能性をもたらす。データの集積に伴うプライバシーを単一システムで収集したデータのプライバシーと比較して見ると、万一悪事を働く人間に利用されることや情報が明らかにされることによるプライバシーへの懸念の深刻さを認識できるだろう

5.1.1.2.デフォルトとしてのプライバシー

2014 年 1 月、連邦取引委員会（FTC）の議長は、IoT の関係者は「セキュリティを製品開発の一部として取り入れること、必要最小限のデータ収集、消費者に消費者データの想定外の利用についての通知とその利用に関する簡単に判断できる選択肢を提供すること」に対する責任を負うと指摘した。IoT の機能を実装する組織は、このことを認識し、そのシステムに、IoT ベンダが提供したデバイスまたはアプリケーション固有のプライバシー管理に加え、（自らの）プライバシー管理を確実に組み込むようにしなければならない。

5.1.2.プライバシーの設計への組み込み

IoT の機能を実装する組織は、まず、関係先からのプライバシーに関する懸念の本質を理解することが必要である。従い、IoT システムが扱うデータ要素が何であるかをはっきりさせるための分析が重要である。これは IoT システムの設計の初期段階で、推奨されている脅威分析と関連させて実施することが理想的である。

データ収集の間接的な影響について精密な解釈ができたら、プライバシーへの懸念が後から指摘されたり事故が起きてから対策するのと比べれば、IoT システムの設計に最初から適切な安全対策を組み込むことができる。併せて、組織は IoT に関連する諸相をカバーする、個人情報漏えいの通知のためのプログラムについて、再度点検しておくべきである。

5.1.3.全機能の発揮：ゼロサムでなくプラスのサムを

機能性とセキュリティの達成目標は相互のバランスが取れるもので、そのバランスを保って、どんなシステムでも正しく動作し、ビジネス要求を満たし、かつセキュアであるようにしなければならない。同じことはプライバシーにも言える。IoT の場合、機能性、セキュリティ、プライバシーのバランスを設計過程の早い段階で達成し、この三つの達成目標を均等に満たすようにすることが特に重要である。IoT システムの運用段階でプライバシー問題を把握することは、プライバシー管理を後付けで導入するプロセスを難しくすることである。

プライバシーバイデザインの原則に忠実に従ってこれら三つの要素のバランスを確認し実装すれば、そのコストは IoT システムの設計にとって比較的軽く済む。

5.1.4.エンドトゥーエンドのセキュリティ：ライフサイクル保護

IoT においては、収集したデータは長い寿命をもつ。収集したデータのライフサイクルの、収集する組織だけでなくその提供先である全ての第三者を含めた全スパンについて考慮することが重要である。関係者は、データが第三者にいつ提供されるのか、そのセキュリティのための管理策、データが廃棄される時期と方法について把握しなければならない。

ライフサイクル保護は、二次データ（一次データに基づいて推測または判断された、個人に関する情報）にも適用しなければならない。例えば、車のセンサーが運転者の運転習慣について、距離、場所、速度その他の属性を収集する場合、第三者がその運転者について様々な推測を出来る。例えば買い物や勤務上の癖や、交際・取引相手などについて。データの所有者（つまり車のメーカ）は、車が売り払われる段階で一時詳報は消すだろう。しかし実態として、抽出された情報（社会的関係や買い物の癖など）は全て残しておくだろう。

5.1.5.可視性と透明性

全ての利害関係者は、すべての IoT システムについて、そこから収集されるデータと、その利用予定および利用の可能性について容易に把握できなければならない。利害関係者はまた、データの収集について大まかなレベルと詳細なレベルにおいて諾否の選択権を与えられなければならない。例えば、あるアプリケーションが運転パターンを追跡する（例えば保険目的で）場合、その利用者はその目的（大まかレベル）に明示的に限定して利用を許可することができなければならない。利用者はまた、希望に応じて個別のデータ、例えば GPS を介しての運転パターンもしくは履歴の蓄積など、について明示的に許可を与えることができなければならない。

5.1.6.ユーザプライバシーの尊重

利害関係者の情報のプライバシーを守ることは、IoT の時代においては、企業にとって実質的に差別化の要件となるであろう。利用者のプライバシーを正しく扱えない場合が非常に多くあることを考えると、機微な情報を保護するのに必要な手立てを講じる組織は、そうでない組織に比べて格段に好ましいものに見えるであろうから。このことを踏まえると、組織の中にプライバシーの文化を浸透させることは重要である。その一つの手段として、プライバシーに熟達した者を一人か何人か配して、IoT システムの実装に際してのプライバシーインパクトを評価させることがある。その任にある者は、プライバシーに関する懸念事項が見つかった場合に設計変更を強制できる権限を付与されることが望ましい。

ユーザのプライバシーはまた、間接的な面からも関係してくる。何かの IoT デバイスにおいて、例えばスマートグラスで、ユーザはプライバシー条項に同意したけれども、見られている者は同意していない可能性が極めて高い。このようなタイプの状況に関して、その影響や必要な規制について、より一層の調査が実施されなければならない。

5.1.7.プライバシーインパクト評価（PIA）

EU の WP29 ガイダンスはまた、プライバシーインパクト評価(PIA)の実施に関する推奨フレームワークを提示している。*[EU]

あるデバイスがプライバシー保護情報（Privacy Protected Information (PPI)）を収集、加工、保存することが確認されたら、より厳格な管理が要求される。この管理はポリシーによるものと技術的なものの組合せであるべきである。例えば以下のものがあげられる。

- デバイスの設置は、より多段階の管理者の承認を要する。
- 内部監査または法令順守管理部門による点検を行い、IoT デバイスが PPI を取得できるかどうか判断しなければならない。
- IoT デバイスに蓄積されるデータは、十分な強度をもった暗号アルゴリズムにより暗号化しなければならない。
- IoT デバイスから送信／受信されるデータは、十分な強度をもった暗号アルゴリズムにより暗号化しなければならない。
- IoT デバイスへの物理的および論理的アクセスは、許可された要員に限定されなければならない。
- 地域により考慮すべき、プライバシーの要求事項についての様々な推奨事項がある。例えば以下のものがあげられる。
- 北米： 連邦取引委員会（FTC）レポート「Internet of Things, Privacy and Security in a Connected World」
  欧州： EU WP29（欧州データ保護勧告機関）「Privacy Recommendations for the IoT」

5.2.新規の IoT システムの構成と配備に際してセキュアシステムエンジニアリングのアプローチを用いること

ある種の IoT の機能は、単に分析エンジンにデータを送り込むセンサーで構成されているに過ぎないかもしれないが、IoT の高付加価値の能力は、複数のネットワークを行き来するデータを活用する多種類の構成要素が数多く働いた結果もたらされるものである。これらのシステムが構成されるに際して、セキュリティ機能がシステムの配備に先立って実装されることを確保するために、セキュリティ要求条件を定義して注入することが重要である。この取組みを実践する標準的な活動は、脅威モデル開発であり、これは従来からあるシステムの設計手法から取り入れることができる。

5.2.1. 脅威モデリング

脅威モデルの開発の方法は Adam Shostack の著書「脅威モデリング：セキュリティのための設計」から学ぶことができる。マイクロソフトもまた、よく考えられた脅威モデリングのアプローチを定義しており、新しいシステムによりもたらされる脅威の深刻度を簡易評価で決めるアプローチを用いている。以下はマイクロソフトのソフトウェアデザインライフサイクルに基づく脅威モデリングの手順である。

5.2.1.1. ステップ 1： 資産の特定

これは IoT システムが配備する様々なコンポーネントをリスト化することである。IoT デバイスだけでなく、デバイスが通信する相手のデータ蓄積デバイスやアプリケーションやシステムとやり取りするユーザも考慮にいれる必要がある。

5.2.1.2. ステップ 2： システムの作成／全体像の構成

このステップは一番の基礎となるところで、IoT システムの予定する機能性だけでなく、攻撃者がシステムをいかに攻撃・悪用するかについて明らかにする。この手順はまず予定する機能性を文章で記述するところから始まり、次に十分時間をかけて、システムの誤用・悪用のケースを記述していく。構成図を作成して、新しい IoT システムの詳細を示し、システムが他の全社的コンピューティング資源やセキュリティシステムとどのようにインターフェイスするかを示すことがまた重要である。この構成図はまた、信頼の境界や認証認可メカニズム、更にはロギングの実施構想を確認するための出発点としても活用できる。

システムアーキテクチャの作成には、ユースケース分析が役立つ。以下の健康医療分野からのユースケースは IoT の実装におけるセキュリティの考慮事項に、示唆を与えてくれる。

1. ある人がある種のモニターを身につけていて、そのモニターはクラウドを介して主治医に情報を上げている状態において：
    a. 緊急の状況において、第一報は自動的に発信されるか？
    b. 新しい薬の処方箋は自動的に（一定のルールの下に）作成され、あるいは処方情報は購入に際して競争相手となるいくつかの薬局に回送されるか？
    c. 医師の診察は自動的にスケジュールされるか？
    d. 医療記録は自動的に更新されるか？
    e. 医療隊が派遣されたら、データは自動的に救急車に転送されるか？

2. 埋め込まれたあるデバイスがある命令を受け取った状況において：
    a. デバイスは PKI に対応しているか？もしそうなら、そのデバイスは命令の送り手に関する失効情報を確認できるか？
    b. デバイスはメッセージの真偽を確認できるか？
    c. デバイスは命令の送り手とセキュアなリンクまたはセッションを張れるか？
    d. デバイスはコンファームを要求できるか？

3. ある医師が、スマートホーム／ホームモニターと通信経路を張った状況において：
    a. 通信チャネルは PKI でセキュリティを確保できているか？
    b. 個人識別情報と医療データはセキュアに送信できるか？
    c. 医師はデバイスに命令を発するか？その場合、その命令の完全性確認とロギングによる否認拒否確認は確保されているか？

4. ある病院が患者の医療記録または分析結果をコンピュータまたは携帯端末に送信する状況において：
    a. 患者は病院のサービスとやり取りが可能か？例えば次の予約を取るとか？
    b. 患者は送られてきたメッセージの真正性を確認できるか？

c. 患者はメッセージをうまく削除できるか？

5. ある患者の献血した血液がオンライン分析デバイスにかけられる状況において：
   a. 献血者の識別番号の保護は端末側かセンター側か？
   b. 患者は分析結果を直接通知されるか？
   c. 患者が STD（性感染症）をもっていた場合、どの機関に通告されるか？
   d. 信頼（trust）のメカニズムは何か？
   e. 血液のパックはロボットが取り扱うか？
   f. 患者のかかりつけ薬局または医師は、分析結果を通知されるか？
   g. メンテナンスセンターは分析デバイスの状態について情報を受け取るようになっているか？

6. （欠番）
7. 緊急事態には、複数の緊急対応チームが派遣される状況において：
   a. 医療情報は該当する救急車にセキュアに伝送されるか？
   b. 救急隊員は患者のデータをセキュアに通信できるか？それは端末間直送かセンタールーティング機能経由か？
   c. セキュリティ、トラスト、プライバシーは複数の「信頼の連鎖」により管理されるか？

8. 製薬メーカが、薬剤注入ポンプデバイスに関する注意喚起を発行した状況において：
   a. 製薬メーカのメッセージを、薬局は信用することができるか？
   b. 注意喚起情報は患者の注入デバイスに影響を与えるか？
   c. 医師は注入デバイスに関する対応処置を出すか？
   d. 薬剤注入ポンプは制御デバイス／モニターとの間で閉回路の通信を行えるか？

9. ある医師がロボットを使って遠隔手術を実施する状況において：
   a. 通信チャネルは信頼でき、セキュアであるか？
   b. ロボットを特定する名前のコンソール上の表示は信頼できるか？
   c. 通信は DNS に依存しているか？
   d. IP VPN で使うアルゴリズムの強度と鍵長は何か？
   e. 全体のトポロジーにおける「信頼の連鎖」と CRL 管理はどのようになっているか？
   f. バックアップ用通信チャネルはプライマリと同等の信頼性レベルがあるか？
   g. 薬剤供給デバイスとその記録はリアルタイム更新が確保されているか？

10. 政府当局が埋め込み型医療デバイスに関する保健通告を発した状況において：
   a. 関係先に対する通知はどの順序でもたらされるか？（医師、薬局、医療メーカ、システム管理者、等）
   b. その通知は証明付きで検証可能か？
   c. あるデバイスがリコールされる場合、どんなデータベースをアップデートする必要があるか？
   d. 在庫管理において、全てのデバイスが適切に管理されるよう担保されているか？

11. ある埋め込み型または装着型デバイスが（訳補：プログラムの）更新を必要としている状況において：
   a. 更新はリモートで実施できるか？
   b. デバイスと中央のサーバの間で相互信頼が可能か？
   c. 通信チャネルはセキュアで信頼できるものか？

d. 在庫管理において、全てのデバイスが適切に管理されるよう担保されているか？
e. 手順もしくは指示内容が変更された場合、全ての関係者に通知が行くようになっているか？
f. 薬剤が関係する場合、関係する薬局に通知は行くか？

12. ある特定のデバイスの担当医が他の医師と交替した状況において：
a. それらの医師の認証情報はデバイス側管理か中央管理か？
b. 医師とデバイスの間には相互信頼の確認手段があるか？
c. 新しい信頼付与のために、デバイスはリモートでアップデートされるか？

13. あるデバイスメーカが遠隔制御型医療デバイスの取扱方法について注意喚起を発した状況において：
a. コンフィギュレーション管理は適切に更新され、すべての関係者がデバイスと取扱説明のバージョンを確認できるか？
b. 医科大学が関係者に含まれているか？
c. コンフィギュレーション管理のために一元管理用データベースがあるか？

14. 車両間通信が行われる環境で、救急車／緊急対応車両が医療班との間で患者の記録を連携する状況において：
a. 通信は PKI で保護されているか？
b. 医療班と救急車の間は相互信頼が可能か？
c. 患者の記録は患者が収容されたら削除されるか？
d. 救急車に搭載されたデバイスは遠隔管理されているか？

15. 埋め込みデバイスを装着したある患者が 119 番通報した状況において：
a. 患者のデータは緊急指令者に提供されるか？
b. 緊急指令者はそのデータを離れた場所にいる医療関係者や医師に伝達可能か？
c. 相互信頼の確立が可能か？
d. 患者の記録は自動更新されるか？
e. 情報は救急車に対してセキュアに通信可能か？

16. 南米で遠隔の医療関係コミュニティ用にプライベートクラウドが配備された状態において：
a. そのインフラはセキュリティ基準を満たしているかを継承するための監査が可能か？
b. そのシステムはリモート接続されたデバイスをサポートしているか？
c. 遠隔の患者との間では双方向の信認が可能か？
d. 関係者の本人性の認証はどのように行うのか？

17. ナノレベルのバイオ医療装置が遠隔接続で配備されている状態において：
a. 中央の装置との間で相互信頼の関係が確立されているか？
b. その体系を構成する個々のコンポーネントは信頼できるか？
c. 復旧されたモジュールに対して、機微な医療情報は保護されているか？（物理セキュリティ）
d. 在庫はセキュアに管理されているか？

論理的なアーキテクチャビューが完成すれば、IoT システムを構成する具体的な技術を認識し調査することが重要となる。これはプロセッサー・タイプや OS のように、IoT デバイスについてのより低層で詳細部分を理解し、文書化することを含んでいる。最終的に公開される特定の脆弱性のタイプを理解し、パッチやファームウェアの更新をどのように、どの程度適用すべきか、そのプロセスを定義するために必要とされる情報を提供する。個々の IoT デ

バイスで使用されるプロトコルを理解し文書化することにより、特にシステムや組織に渡って送信されたデータに適用された暗号の中にギャップが見つかった場合、アーキテクチャへの変更も許可される。

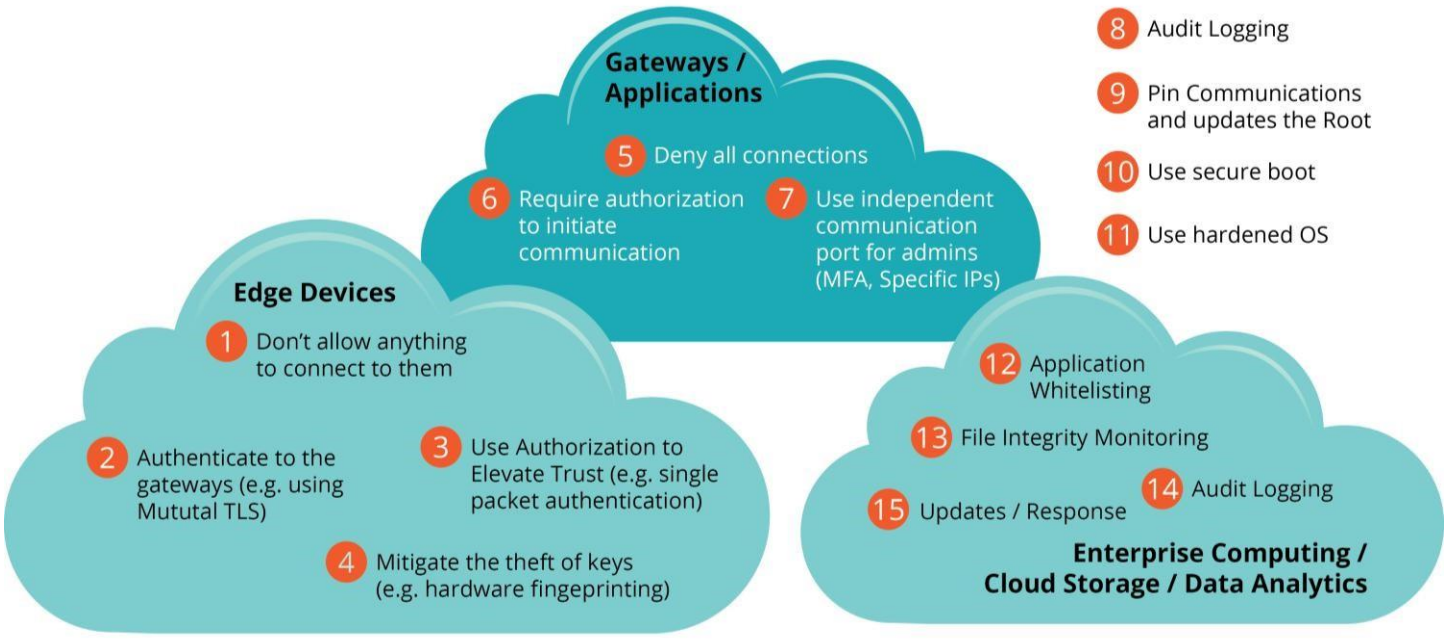
5.2.1.3. ステップ３： IoT システムの解析

このステージでは、データがシステムの中を流れるライフサイクルの理解に焦点を当てる。この理解を得ることは、セキュリティアーキテクチャの中で確認すべき脆弱な点を特定するのに役立つ。システムの中でデータの入るポイントを突き止め文書化する。IoT システムにおいては、これらの入り口は往々にしてある種のセンサーである。データの流れを入口からトレースし、システムの中でそのデータとやり取りする様々なコンポーネントを書き留める。攻撃者の目につきやすい標的を特定するーそれはシステムの中でデータを集積または保存するポイントであるか、重要なセンサーでシステムの全体的完全性を維持するために厳重な保護を必要とするものである。この取組みをすることで、新しい IoT システムの攻撃対象面をよく理解することができる。

5.2.1.3.1. ステップ３a： 防御アーキテクチャの決定

IoT システムの解析ができたら、次のステップはシステムを保護するためのアーキテクチャの設計になるだろう。概念的な防御アーキテクチャを適用すべきである。そこには SDP のいくつかの要素が適用される可能性がある。Junaid 氏のコメントに基づき、IoT 環境に適用できる概念的ダイヤグラムを示してみた。いかがであろうか。

IoT の防御アーキテクチャの構成要素



IoT 環境の保護のための概念的アーキテクチャができたら、脅威をリスト化し、以下のように詳細なガイダンスを提供しよう。

5.2.1.4. ステップ４： 脅威を特定し文書化する

よく使われる STRIDE*モデルが IoT システムの実装にも適用できる。環境をよりよく理解するには、よく知られている脆弱性リポジトリ、例えば MITRE の Common Vulnerabilities and Exposures*データベースを用いるのがよい。以下の脅威タイプのリストに拠れば、個々の IoT 構築に固有の脅威を発見することができる：

脅威のタイプ	IoT に関する説明
ID スプーフィング	システムを調査して機会の ID のスプーフィングと、攻撃者がデバイス間の自動化されたトラスト関係を破る可能性に関する脅威を調べること。
データの改ざん	IoT システムの全体にわたってデータのパスを調べること。データの収集、加工、移送、保存の各ポイントにおいてデータを改ざんする機会が生じるポイントを特定すること。
否認	重要なデータを提供するシステム内のノードに関するシステムデザインを検証する。それは多くの場合センサーのセットで、分析用のデータを提供する。IoT の場合、データをそのソースまでトレースバックして、データの供給元が間違いなく想定したソースであることを確認できることが重要である。IoT システムを調べて攻撃者が悪性のノードをしかけることを許し、そのノードにより不良なデータがシステムに供給されてデータ収集プロセスを混乱させたりシステムを正常運転できなくするような、脆弱性がないかチェックする。IoT システムで想定している機能を攻撃者が悪用できないことを確認する。例えば違法な運転が無効にされるか拒否されるように。ステータスの変更や時刻の変動（例：メッセージシーケンスの破壊）に対して注意する必要がある。
情報開示<流出>	IoT システムの、バックエンド処理システムも含む全システムについてデータのパスをチェックする。機微な情報を処理する全てのデバイスが特定され、情報の開示<流出>に対処できるよう適切な暗号処理が実装されていることを確認する。IoT システム内のデータストレージノードを特定し、保存中のデータの暗号処理が適用されていることを確認する。IoT システムをチェックし、IoT デバイスが物理的に盗まれるような脆弱性の事例を調べ、例えば鍵抹消(key zeroization)処理などの適切な防御策が講じられているか確認する。
特権の設定	IoT システムを構成する各種 IoT デバイスに対する管理権限をチェックする。認証レベルが単一で、その権限でデバイスの詳細な設定ができる。他のケースでは、管理者ごとにできることが明確になっている場合がある。IoT ノードの中で、ユーザレベルの機能を管理機能と分離する機能が脆弱であるものを特定しなければならない。IoT ノードが備える認証方法の弱点を特定し、適切な認証制御をシステムの設計に取り入れなければならない。
物理セキュリティの迂回（bypassing）	各 IoT デバイスが提供する物理的防御のメカニズムを調査し、可能な場合は、確認された脆弱性に対する軽減策を計画する。これは特に、IoT を公共の場所や離れた場所に設置する場合には大事である。

脅威のタイプ	IoT における対策
ソーシャルエンジニアリングによる侵入	ソーシャルエンジニアリングに対する耐性訓練をスタッフに施し、疑わしい振る舞いがないか常時資産を監視する。
サプライチェーンにおける問題	IoT デバイスやシステムを構成する様々な技術的構成要素を理解し、これらの技術階層のいずれかに関わる脆弱性への追尾をし続ける。
ネットワークへの侵入	ネットワーク上の疑わしい動きを常時監視する。

5.2.1.5.ステップ５：　脅威のランク付け

上記のステップを通じて特定された各脅威の発生可能性とインパクトを評価すると、各脅威に対応するための適切な投資レベルが得られる。高いリスクにランク付けされた脅威は、即時に対処する必要が高い脅威である可能性が高いのでより多くの費用が必要になると考えられる。この段階では、標準的な脅威のランク付け方法を用いても差し支えなく、その方法にはマイクロソフトの DREAD アプローチも含まれる。

5.2.2.セキュア開発

IoT のエッジデバイスは、ハードウェア、オペレーティングシステム（OS）、ファームウェア、ソフトウェアの組み合わせである。これは、新しいデバイスを作りだす時には、ベンダは、これらテクノロジースタックの全てのレイヤーにおけるセキュリティの脆弱性に気をつけなければいけないことを意味する。これには、例えばベースとなる OS の強化（可能な場合）や、プラットフォームのハードウェアに特有の脆弱性の除去が含まれる。エッジにおける IoT デバイスはまた、他の多くのデバイスやシステムと接続するので、実際問題として System-of-Systems を創り出している。エッジデバイスのいくつかは、これらのフレームワークや OS やプラットフォームの上に乗る非常に限られたコードで成り立つ。一方、より複雑なエッジデバイスもあり、このような「もの」は、従来型のエンタープライズまたはモバイルアプリケーションと同様のセキュアソフトウエア開発規範を多く取り入れなければならない。その例としては、静的および動的コード解析ツールを用いてのコード脆弱性分析や、修復対象となるソフトウェア脆弱性発見のためのペネトレーションテストの実施がある。

OWASP (Open Web Application Security Project) は IoT デバイスメーカー向けにセキュア開発ガイダンスを提供している。OWASP の IoT トップ 10 には、IoT デバイスを開発するに際して対処すべきセキュリティ上の課題が示されている。例として以下のものがある。

- セキュアでないクラウドおよびモバイルの API
- 転送時の暗号化の欠如
- 不十分な認証と認可

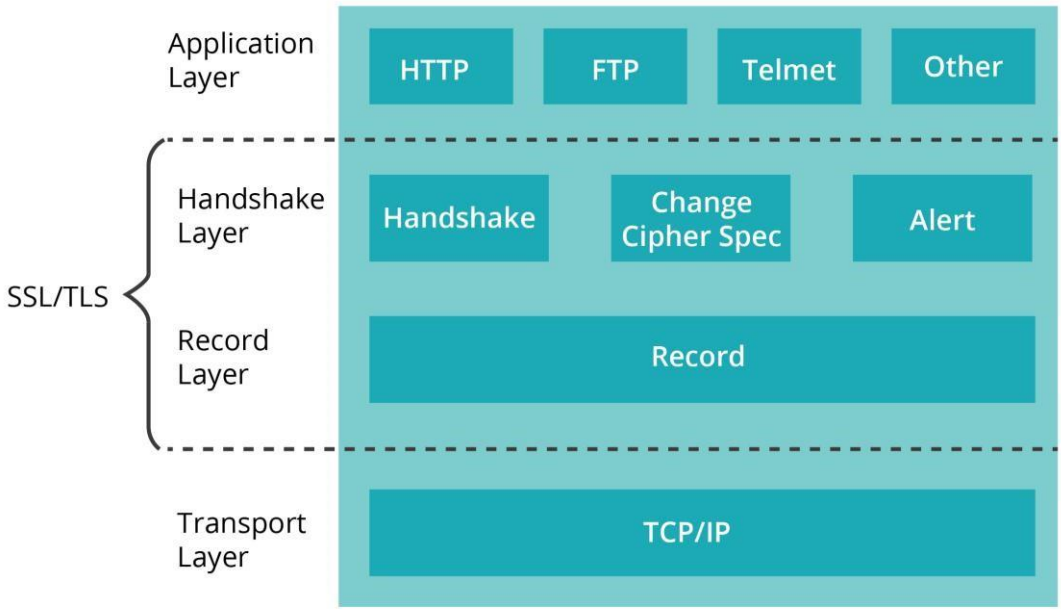
IoT ベンダにとって、セキュリティエンジニアリング能力を確保し、セキュアな IoT ソリューションを設計できるようにすることは重要である。社内にこの能力を備えることは、新しい課題を背負うことになる。なぜなら

セキュリティの規律や考え方を身につけ脆弱性を発見できるようにスタッフを教育するコストは高いものにつくからである。”Builditsecure.ly”や”I am the Cavalry”といった組織は、それを実現するためのガイダンスを提供している。しかし一方、IoT の開発者にとって興味ある別のアプローチとしては、独立のバグハンターのクラウドソーシングを活用するということがある。”BugCrowd”のようなサイトは、開発者に第三者のセキュリティアナリストによるコードレビューを提供したり、更には場合によっては、ハードウェア実装のレビューまで行い、発見した脆弱性を示してくれる。

IoT のセキュア開発の方法論を開発している組織は、セキュア開発のフレームワークを定義づけることを考えるべきである。フレームワークでは、組み込みソリューションやパラメーターの設定・調整や API のセキュアコーディングの手法を詳細に記述するべきである。IoT 向けのこれらのセキュアコーディング手法を開発するには、REST や SOAP/XML が提供する API セキュリティベストプラクティスを活用するとよい。併せて、通信に用いる各種プロトコルや、IoT デバイスの様々な利用者に割り当てられるアクセスレベルに伴うセキュリティリスクについても詳細に記述するべきである。

IoT の実装に適用する適切なセキュリティコントロールを理解するための大事な要素は、利用するデータリンク層とトランスポート層のプロトコルセットである。IoT に用いられる各種のプロトコルの各々は様々なレベルのセキュリティをサポートし、そのいくつかは組み合わせることで十分にセキュアなコンフィギュレーションを提供する。IoT システムの設計者として、組織は、これらのプロトコルを理解し、さらに一つのプロトコルを使うことはより高いレベルのプロトコル、例えば機密性と認証のための TLS (Transport Layer Security) プロトコルの利用の必要をもたらすということを学ぶことになる。Appendix A は利用可能な様々な IoT プロトコルについての見取図を示している。

SSL, TLS Protocol Layers



他に考慮すべきことは、通信用およびセキュリティ用のプロトコルを実装するのに使うツールそのものをよく調べる必要があることである。例えば、”Heartbleed”バグは 2014 年 4 月に発見されたが、TLS の OpenSSL 部分にだけ関係するものだった。SSL は web サイトとユーザ間の暗号通信に用いられる暗号プロトコルである。OpenSSL における input チェックが正しくなかったために、Heartbleed バグによって、ハッカーは OpenSSL を使うサーバから web ユーザの高度に個人的情報を抜き取ることができた。他の TLS に関するプロトコルの実装は影響を受けなかった。（例えば Microsoft, Mozilla, GnuTLS には影響がなかった。）今日でもなお、多くの脆弱な OpenSSL のデバイスはパッチが施されていない。スキャニングツール Shodan の開発者である John Matherly の分析によれば、2014 年 12 月現在、30 万のデバイスはパッチがあてられていないことが突き止められている。その多くが「組み込み型」デバイス、例えば web カメラ、プリンター、ストレージサーバ、ルータ、ファイアウォールなどである。

5.2.2.1.セキュアサプライチェーン

IoT の技術スタックのレイヤーが異なると、往々にして異なるサプライチェーンの諸相ーハードウェア、ファームウェア、OS、プロトコル、クラウドプロバイダなどーに直面することになる。これらレイヤーの各々と関わることは、しばしばある特定のインテグレータの製品だけに固有の脆弱性となって現れることがある。デバイスを提供する製造業者は、ODM (Original Device Manufacturers) 業者に対してデバッグインターフェイスと不要のアプリケーションを業者の出荷前に削除することを義務付ける文章を、サービスアグリーメントの中に加えるべきである。もしサプライチェーンを構成するベンダが、製品の中で自社の責務として機能試験といじめ試験<positive and negative tests>を実施すれば、各上位の開発者は、最終のアプリケーションの開発の流れの中で、そのテスト結果を自社の IoT デバイスに使われる下位の基盤部分がセキュアであることを検証することができる。これらのテストはひとまとめにしてダウンロードできやすくし、反復組合せテストに際してテスト自動化ツールによって実施しやすくすることが望ましい。例えば、ある開発者が外部の TLS 実装を利用する場合、その TLS ライブラリは、自動実行可能なコンフォーマンステストのスイートとともに提供されるべきである。

IoT 製品を購買する組織はまた、サプライチェーンの能力をしっかりと監視し、最新版のファームウェア、ソフトウェア、パッチを提供できるよう計画すべきである。望むらくは、これは IoT デバイスベンダーとの間のライセンス契約に盛り込まれるべきである。

5.3. IoT 資産を防護するために階層化したセキュリティ保護を実装する

IoT はエコシステム内の既存の IT と運用技術(OT)[2]のネットワークを、何百万というセンサー、デバイス、その他のスマートオブジェクトと融合する。このことは、既存のネットワーク経由の結合を広さの面でも深さの面でも拡大するために、セキュリティにとっての課題を著しく膨張させる。

[2] Operations Technology：企業の管理業務用の IT（エンタープライズ IT）ではなく、ビジネス現場で主に使われる技術やシステム（たとえば、製造システムやサービス用システム）を指す。多くの場合、これらの技術は IT 部門から切り離されて、現業部門が導入、運用に責任を持つ。

IT と OT のネットワークは、各々意識の中で違う優先度で管理されており、かつ各々が明確なセキュリティのニーズを持っている。IT ネットワークの優先課題はデータの機密性の防御である。OT ネットワークの焦点は物理セキュリティであり、運転上および従業員の安全確保にある。

これら 2 つの環境の融合の結果、IoT のセキュリティは物理的とサイバーのセキュリティの要素を組み合わせた新しいアプローチが必要となる。その結果、従業員のセキュリティは改善され、システム全体の外部と共に内部に対する保護が可能となる。

デジタルの世界で活動する組織は今日では階層化されたセキュリティが必要であり、その結果、ファイアウォールを通過する e メールメッセージはメールサーバのアンチウイルス機能により停止させられ、そこを通過すると、次にはワークステーションのアンチウイルスによって停止させられる。悪意あるプログラムがワークステーションに足掛りを確保しようとすると、それがワークステーションで走る時に疑わしいもしくは想定外の動作をすることで検知される必要がある。インターネット上のサイトへの既知の有害な行為を伴う接続を見張り、ファイアウォールの外向けフィルタリングでそのようなサイトをブロックする。

攻撃者は web アプリケーションや、OS や、更にはより深くハードウェアまで覗き込むために、全力を尽くします。。彼らは旧式のエンドポイントやモバイルデバイスを利用して過去のもしくは通過型のネットワークセキュリティをすり抜け、更にはデバイスを運転する人の人的要素も利用する。

設計段階では、IoT アーキテクチャの脅威モデルに関して慎重に考慮を払い、以下に記述する全てのレイヤー（デバイスレイヤーを含む）において、関係する人とその役割、使われるコンポーネント、データの入出力ポイントを考慮対象としなければならない。様々な脅威シナリオを、数知れない誤操作のケースについて考え抜き、開発／ビルドのチームに引き継ぎ、開発／ビルド段階での実践規範を盛り込み、セキュリティテストを実施しなければならない。IoT の利用者の視点からは、IoT の取組みが実施に移される前に、徹底した計画が練られなければならない。これらすべてのレイヤーにおいて、セキュリティニーズは注意深く考え抜かれなければならず、フルにセキュアな実装を確実にするには、一つや二つのレイヤーだけでは不十分である:

5.3.1.ネットワークレイヤー

- ファイアウォールはタイプ、ポート、送付先に基づいてトラフィックをフィルタするように設計されている。ファイアウォールは IPS やトラフィック検査サービスのようなより深い分析を取り込むことで進化し、パケットをより深く観察し、悪意あるトラフィックを検知できるようになった。このようなデバイスは、多層防御を実装するに際しての最も容易な出発点である。
- ファイアウォールとルータの開けてあるポートを頻繁にスキャンする必要がある。開いているポートはハッカーへの招待状のようなものである。
- ルータが NAT-PMP (NAT-Port Mapping Protocol) サービスの設定ミスに対して脆弱かどうかチェックすること。NAT-PMP は、組み込まれた認証メカニズムを持たず、ルータのローカルネットワークに属する全てのホストを信用するプロトコルで、ファイアウォールを通して攻撃者が自由に「穴」を開けることを許してしまう。NAT-PMP に対して設定ミスのあるルータは OWASP の「IoT の 10 大脅威*」で取り上げている。

- アンチウイルスやホスト IPS などのエンドポイントセキュリティ技術を統合するために、NAC (ネットワークアクセス制御)を実施すること。例えばアンチウイルス製品は、ファイルのシグネチャとの比較を用いてコンピュータをマルウェアから保護する。
- 脆弱性検査を定期的に実施して、ネットワークに対するユーザとシステムの認証のどちらも組織のセキュリティポリシーに準拠していることを確認すること。これには、パスワードの強度を高くするポリシー、パスワード管理及び定期的なパスワードの変更が含まれる。
- ルータやゲートウェイなどのネットワークデバイスにおけるゲスト用およびデフォルトのパスワードを無効化すること。これは新しいネットワークデバイスを開梱し、それらがネットワークに投入される前に実施すること。
- 全ての MAC アドレスを記録し、ルータがそこに記録されているデバイスだけに IP アドレスを割り当てるようにすることはよいやり方である。全ての未知のデバイスはネットワークへのアクセスをブロックされることになる。
- 無線ネットワークには、WPA2 (Wireless Protected Access 2) を用い、WEP (Wireless Encryption Protocol) を用いないこと。WPA2 はより強い暗号化を要求する。無線ネットワークでは、常に強い複雑なパスワードを用いること。
- 無線ネットワークではまた、単一でなく、複数の SSID (Service Set Identifiers) を用いること。これにより、ネットワーク管理者は各 SSID に別のポリシーと機能を割り当てることができ、組織がリスクと重要度に応じてデバイスに別々の SSID を割り当てることを可能にする。このように無線ネットワークをセグメント化することで、例え一つのデバイスがハッキングされても、他のデバイスは別のセグメントに要るために影響を受けないということが可能になる。
- PPSK (Private Pre-Shared Key) を用いて各センサーやデバイスが Wi-Fi にセキュアに接続できるようにすること。管理者はネットワーク上の各クライアントに、個別の取り消し可能の鍵を割り当てることができる。これらの鍵は、その鍵を使って接続しているデバイスに、このような許可を与えるかを特定できる。このようなことを実現する技術を提供する会社がある。

- IoT デバイスは、ますます多くのデータを分析のためにクラウドにため込んでいる。このデータを暗号化や他の手段を使って適切に安全を確保することが重要である。（例えば、患者をモニターしているデバイスからの機微な情報をクラウド上のストレージに送ることなど）

5.3.2.アプリケーションレイヤー

IoT には、全く新しいアプリケーションセキュリティとベストプラクティスのセットが必要な訳ではない。従来型の実装に使われるアプリケーションレイヤーのガイドラインが通用する。

- ある組織がその独自のアプリケーションを書く場合は、適切な認証と認可のメカニズムを用いること。全ての平文のままのパスワードとアプリケーションコードの中にあるパスワードを洗い出すこと。（例：ハードコードされた telnet のログインやテストの際に使用したまま放置されているパスワード）
- 第三者もしくはオープンソースのライブラリを使っている場合は、それらのライブラリのリストを作成して、常に最新の情報に更新しておくことを推奨する。同時に、バージョンとそのバージョンに該当する脆弱性をチェックし、そのような脆弱なバージョンを使わないようにする。これにより、使われている第三者のもしくはオープンソースのライブラリにセキュリティパッチが当てられていることを確実にすることができる。
- 全てのクロスサイトスクリプティング（XSS）またはクロスサイトリクエストフォージェリ（CSRF）脆弱性を確認すること。CSRF は、悪意を持ったウェブサイト、e メール、ブログ、IMS またはプログラムに

よる攻撃で、信頼できるサイトにおいてブラウザに意図せざる動きを行わせる。XSS は攻撃者が、他のユーザが見るウェブページにクライアント側のスクリプトを埋め込み、またはアクセス制御をバイパスできるように働く。OWASP は ZAP (Zed Attack Proxy) や DAST (Dynamic Application Security Testing) のようなスキャニングツールを使うことを薦めている。

- IoT プラットフォームの開発過程で発見された脆弱性についてのセキュリティコードレビューレポートと、それに対応する解決策をベンダに要求すること。このステップは SAST (Static Application Security Testing) の観点からは詳細検査(due diligence)として機能する。もし IoT プラットフォーム上でホストされるアプリケーションを開発しているならば、そのアプリケーションに対しては、DAST と並んで SAST も実施しなければならない。
- アプリケーションは、他の組織によって管理されたり、ホスティングされたり、あるいは、サービスの形で提供されることがある。利用者がサービスのデフォルトパスワードを変更するように教育すること。
- セキュアでないクラウドのインターフェイスは OWASP の IoT10 大脅威に示されている。https が必ず使われるようにすること。また認証のリトライの規定回数を超えた場合やタイムアウトした場合のロックアウトを強制実施すること。
- 保存中のデータは暗号化すること。転送中のデータのプライバシーを強力な暗号を用いて確保すること。ハッキングを困難にするために、ハッシュ値に salt やランダムデータを付加すること。
- 移送中のデータの暗号化は、リソースに制限のあるデバイスについて配慮できるものでなければならない。従い、ボトルネックを避けるために、従来型の暗号と違って、データ量が少なくかつ処理負荷の小さいものにしなければならない。
- 「正常な振る舞い」をベースラインにすることで、異常な振る舞いを後から検知できるようにすること。通信トラフィックのベースラインにはファイアウォール、ルータ、スイッチ、通信収集デバイス、ネットワークタップが該当する。ファイアウォールやルータはトラフィックを通過させるので、起点としては理想的である。セキュリティの観点から最も典型的に関心の対象となるのは、内部のホストとインターネット上のホストの間のフローである。
- IoT デバイスの web アプリケーションに特有の課題の一つに、通常使われる 80 番や 443 番でない、非標準のポートが使われる傾向があることがある。デバイスは他のポートを聞くように作られている。あるデバイスの web サービスが何を提供するのかを知るには、標準的なポートスキャナーや shudder を使うのが最も良い。IoT デバイスの非標準ポートをスキャンすること。なぜならそれらは標準ポートを使わない場合があるから。

使われる可能性のある攻撃メカニズム以外に、IoT デバイスの物理的インターフェイスの更なる保護が必要な場合がある。JTAG や不要なシリアルその他の製造者用インターフェイスは、量産開発の前に削除するか改ざん防止措置を施すかするべきである。非公開鍵または秘密鍵は不揮発メモリの中で動作し、承認されたユーザだけがアクセスできる”secure element”チップに格納するべきである。

5.3.3.デバイスレベル

デバイスの例としてはセンサー、データを集積するゲートウェイ、モバイルデバイス、カメラ、RFID リーダ、ウェアラブルデバイス、埋め込み型デバイスがある。産業によっては、他の産業と共通性のないデバイスもある場合があり、従ってこのリストは特定のデバイスに関する固有のガイドラインを欠いている可能性がある。

デバイスのファームウェアが、定常的にアップグレード、アップデート、パッチを確実に適用されるようにすること。

- アップデートファイルの供給元とそれがどのように伝送されるかについて確認すること。デバイスにそれをインストールする前にファイルのスキャンもしくは完全性のチェックを確実に行うこと。ファイルの「評判(reputation)」を確認すること。方法は色々ある。全てのコンピュータファイルは固有のチェックサムーそのファイルに対応した比較的短い数学的値を持っている。ファイルの評判に関わる他の特性として、それがどれだけ広範囲に使用されているかがある。そのように評価すれば、ファイルに関する経歴が得られ、それがよいものか悪いものかの情報や詳細に監視すべき未知のリスクがあるかがわかる。
- Bluetooth デバイスのデフォルトの接続用パスワードを変えること。
- デフォルトのパスワードを変更し、強度の高いパスワードポリシーを適用すること。
- パスワードだけでなく、デフォルトの設定を変えてデバイスを強固にすること。
- デバイスを配備する前にテストすること。”Fuzzing”ツールはデバイスに想定外のデータを送り、その反応によって潜在する不具合を検出する。
- モバイルデバイスでは、指紋認証によるアクセス制御の方が強度は高い。アイドル（無操作）時間と認証失敗回数によるロックアウト機能を実装すること。
- デバイスとセンサーは定期的にテストして適正に機能することを確認しなければならない。
- 医療分野では、ペースメーカーのような装着型デバイスと埋込み型デバイスは攻撃に対して脆弱で、攻撃は無害な盗聴から致命的な攻撃まである。攻撃者は無線で認められていないコマンドを送りつけたり、またはサービス不能攻撃を仕掛けてデバイスのバッテリを消耗させたりする。このようなデバイスを致命的な誤作動から保護するには、ジャミング防止デバイスを装着して攻撃者がデバイスと遠隔地の端末の間に無許可のワイヤレスリンクを張るのを阻止することを検討すること。そのようなデバイスは“装着型シールド”と言う。医師などの許可された者はアクセスでき、他の者はできないことをテストすること。

5.3.4.物理レイヤー

高度に規制された業種では、IoT 以前でも長年にわたり、物理レイヤーのセキュリティは必須であった。例えば、電力およびエネルギー企業は、ミッションクリティカルなデバイスやデバイスに通じるロビーやドアにアクセスできる人物について非常に厳格である。なぜなら一つの事故が壊滅的停電または思い罰金につながるからである。同様に、IoT の推進で使われるデバイスやセンサーでは、同種の脆弱性が問題になる。OWASP は IoT の 10 大脆弱性の中で物理セキュリティの欠如を列挙している。

- 論理システムと同様、物理的アイデンティティ・アクセス管理インフラストラクチャのガバナンスがあるべきである。データセンター、ラボ、ミッションクリティカルなデバイスがある区画のようなセキュアな領域へのアクセスは許可されたものに限られるべきである。バッジの着用はアクセスを最も制限する。
- 物理的な鍵はセキュアトークンと同様慎重に配布すべきである。
- モニター用カメラを用いて区域に配備されたデバイスを常時監視すべきである。デバイスやセンサーが実装されている区域をスキャンするために、カメラは左右に振る機能が付いているべきである。
- デバイスの設置場所を文書化すること。できれば、ビルの中で IoT デバイスが設置されている場所を示す見取り図を作成すること。

物理サイト（室内、屋外）や設置場所（保護されたサイト vs 保安員のいないサイト）の多様性を考えると、収納筐体や物理的格納オプションや物理セキュリティ管理は IoT のセキュリティにとって重要な要素であ

る。デバイスの多くは小さく、価格面の圧力は極めて大きい。例えそうであれ、破壊防止容器や破壊への応答および記録メカニズムを、多様な種類の物理的脅威にさらされる程度に応じて検討すべきである。格納容器に、組み込みデバイスの付属部品（例：非常用 CPU/メモリ子ボード）もしくは暗号モジュール（できればハードウェアの）といった破壊対策を装着することも考えられる。デバイスが可動型の環境になく壁や柱や他の台に固定されている場合には、故意の取り外しの検知デバイスを用意して管理者の無許可の取り外しや窃取を知らせることを検討すべきである。

5.3.5. 人的レイヤー

人のレイヤーはセキュリティ上最も困難で、リスクの軽減に関して最もグレーな領域と言える。悪い方に働く要素は多数あり、それを白黒であらかじめ決めつけることは困難である。下記のガイドラインは、組織の投資意思の強さ次第で軽くまたは重みをもって検討する対象である。全体としてここで最も重要なのは、セキュリティ意識のカルチャーの醸成であり、仕事への取組みに際しての意識、説明責任、対応責任を植え付けることである。

- セキュリティのエバンジェリストである数人のリーダを任命すること。これらの人々は人格的にまた推進力の上で、IoT への取組みを最少のセキュリティ課題成功裏に推進する先頭に立てる者であるべきである。
- 継続的にスタッフを教育し、うますぎる話や合法的なビジネスの依頼に見せかけた誘いに乗るようなことがないようにすること。
- デバイスのパッチをダウンロードするのと同様に、従業員はインターネットからダウンロードする際評判を確認するように教育されるべきである。
- 従業員を教育し、各自のモバイルデバイスをセキュアにする方法、例えば上述のロックアウトやパスワード強度を学ばせること。使わない間は Bluetooth をオフにすること。紛失したモバイルデバイスは直ちに届け出ること、また返ってきたモバイルデバイスは検疫を行い、悪用の痕跡がないか検査されるようにすること。
- 脆弱性を発見した従業員を報償すること。
- 従業員だけでなくすべてのエンドユーザが気軽に脆弱性を届け出らけるようにすること。ポータルサイトに報告用のインターフェイスを設けること。報償の仕組みを用いると報告に向けた積極性が生まれる。
- IoT 資産とそれが収集する情報の種類をリスト化すること。それを重要度でランク付けし、よりミッションクリティカルなものに重点が置かれるようにすること。これは、特に全ての IoT デバイスが同等の注意を払われるとは限らない場合には、リスクベースアプローチを用いることになる。
- ベンダやサービスプロバイダに対応して、より高度の基準を拡大適用し義務化すること。

これらすべてのレイヤーについて、IoT 利用者の視点から論じてきたことに留意すること。しかし、IoT デバイスの製造者も同様にこれらのレイヤーについて知り、そうすることで利用者と同じ土俵に立ってその製品を強化できるようにすべきである。デバイス製造者はデバイスレイヤーそのものだけに注目するかもしれないが、責任を持つ必要があり、セキュリティを強化すべき他の領域について利用者が気付く手助けをする必要がある。

結論として、予防が重大なインシデントを回避するベストの道である。各レイヤーにおけるこれらのセキュリティガイドラインが真剣に考えられるほど、IoT への取組みはよりうまく行く。

5.4.データ保護の実践規範を実装して機微な情報を守る

色々な状態にあるデータの保護には暗号の適用が必要である。数多くの暗号利用形態（暗号化、完全性、認証等）が暗号化ソフトまたはファームウェアライブラリもしくはハードウェアモジュールの形で多様に供給されている。NIST（米国国立標準技術研究所）からは機微情報保護用のアルゴリズム、手法、鍵長に関する推奨が提供されている。アルゴリズムと鍵長は IoT の暗号化システムで設定した保護の一番低いレベルに基づいて選択すべきである。

情報保護に用いる暗号化スイートを選択する際の二つの基本的要件として、セキュリティレベルとパフォーマンスがある。パフォーマンスは、IoT で一般的な、典型的には組み込み型のような、制約の多いデバイスでは、特に重要である。ECC（楕円曲線暗号）は小さい非対称鍵ながらも、以下の用途に強力なアルゴリズムを提供する：

- 暗号鍵の生成（Elliptic Curve Diffie-Helman – ECDH 楕円曲線ディフィーヘルマン）
- メッセージ／データへの電子署名（Elliptic Curve Signature Algorithm – ECDSA 楕円曲線電子署名アルゴリズム）

AES (Advance Encryption Standard) のような非対称アルゴリズムと組み合わせると、この暗号化スイートは優位性の乏しいデバイスに適した保護を提供してくれる。

IoT デバイスの内部でサポートすべき暗号アルゴリズムと鍵長を特定することは、暗号適用パズルの一つの側面に過ぎない。これらのアルゴリズムは信頼できる環境の中で動作しなければならず、鍵はセキュアな収納場所に格納されなければならない。規模の大きいシステムでは、設計者はよく鍵の格納と利用に HSM (Hardware Security Module) を採用するが、HSM はしばしば IoT とは両立しない。代替として、設計者は TEE (Trusted Execution Environment) や TPM (Trusted Platform Module) といった他のオプションを探し出さなければならない。

IoT デバイスや管理システムやデータ収集システムで使われる暗号の実装は、暗号アルゴリズム評価テストを受けるべきで、さらに可能なら NIST の CMVP (Cryptographic Module Validation Program)や CAVP (Cryptographic Algorithm Validation Program)といった評価テスト制度による適合性テストを受けるべきである。

5.4.1.データの特定、クラス分け、セキュリティ

IoT の機能を利用しようとする組織は、第一に、データ保護のためのアプローチを含む企業レベルのデータセキュリティポリシーを定める必要がある。このプロセスは、データ要素、それに対応するクラス分け、その他のデバイスまたはアプリケーションの属性を特定するという特別な任務から始まる。データのモデルは IoT デバイスがアプリケーションの一部として伝送し受信し保存する明確に定義された情報をリストするだけでなく、見た目にはあるいは単独では機微であったりプライベートとは見えない物理世界由来のデータもリストし集めなければならない。物理的計測値やデバイスの利用度の測定値なども収集して、データのセキュリティ・データの保護のポリシーがそのアプリケーションだけでなくデバイスの利用パターンに適合していることを確認しなければならない。これは（アプリケーションデータとデバイスの利用パターンに関する）「データオーナーシップ」のポリシーと申告を実現するための厳格な必要条件で、以下のものを必要とする。

- Data At Rest (DAR) Security　保存データのセキュリティ
- Data In Transit (DIT) Security　伝送データのセキュリティ
- Data In Use (DIU) Security　利用中のデータのセキュリティ
- Data Loss Prevention (DLP)　データ漏えい防止
- Data Integrity and Aggregation Policies データの完全性と集積のポリシー

5.4.1.1. Data at Rest (DAR) Security　保存データのセキュリティ

IoT デバイスの複雑度に応じて、アプリケーション固有のデータ要素は、実行プロセスで実際に使われていない場合は暗号化しておく必要がある場合がある。デバイスはこれらのパラメータを、デバイス内の物理的に補強されロックされた暗号モジュール内に安全に保存された DAR 暗号化鍵を用いて暗号化するべきである。機微なアプリケーションデータだけでなく、全ての秘密鍵および非公開鍵や、認証・アクセス制御その他のセキュリティ設定は、可能なら暗号化すべきである。保存データのセキュリティはデバイスの盗難または紛失に際してプライベートな情報（例：医療データ）を保護すべく設計されている。

5.4.1.2. Data in Transit (DIT) Security　伝送データのセキュリティ

伝送中のデータ(DIT)は、リンクまたはネットワーク上で送信しまたは受信する（アプリケーション、管理用コマンド、ステータス等の）データを指す。DIT の保護は、暗号による機密性（暗号化）、完全性、認証のアルゴリズムを含むべきで、そのアルゴリズムは適切に実装された暗号モジュールによって実施されるべきものである。きちんと検証されたネットワークまたはアプリケーションセキュリティプロトコルを可能な限り活用し、エンドトゥーエンドの DIT セキュリティを実現すべきである。

共通鍵が IoT デバイスに予め安全に格納されていない場合、デバイス制御およびデータ収集システムは、デバイスに出入りするデータを暗号化するためのワンタイムまたは短期利用鍵を設定しなければならない場合がある。この目的には完全に一時的または静的な Diffie-Helman 鍵交換（相互認知のデジタル認証値を用いる）が有効で、完璧な送信秘密を確保しつつ暗号鍵を提供できる。

5.4.1.3. Data In Use (DIU) Security　利用中のデータのセキュリティ

IoT のエッジデバイスでのデータ保護では、コードの実行のための信頼できる環境が必要である。これはデータの機密性と完全性の両方を含む。TEE (Trusted Execution Environment) はこの機能を提供し、各種のプロセッサで利用できる。ARM ベースの IoT デバイスは信頼環境での実行のために更に TrustZone といった技術も利用できる。他のアーキテクチャやシステムオンチップ（SoC）や特定の基板による IoT デバイスでは、これに加えて、信頼できる実行のための論理的や物理的な構成を追加できる場合もある。組込型のマイクロコントローラはセキュリティフューズを用いてフラッシュメモリの実行環境や重要なデータもしくは設定を外部からいじることを防ぐべきである。マイクロハードウェアベースのセキュリティ保護に加え、可能な場合には、WindRiver などのセキュアな OS の利用が推奨される。IoT デバイスの多くはその形が小型で能力の高い SoC ユニットになり、各種のセキュアブート可能な OS を走らせることができ、厳格なアクセス制御や信頼実行環境や高セキュアなマイクロカーネルやカーネル分離やその他のセキュリティの機能を提供できる。セキュアな、正式にモデル化されたマイクロカーネル、例えば NICTA (National ICT Australia) seL4 は、IoT デバイスをゼロから構成する際に強力な基盤を提供してくれる。

5.4.1.4. Data Loss Prevention (DLP)　データ漏えい防止

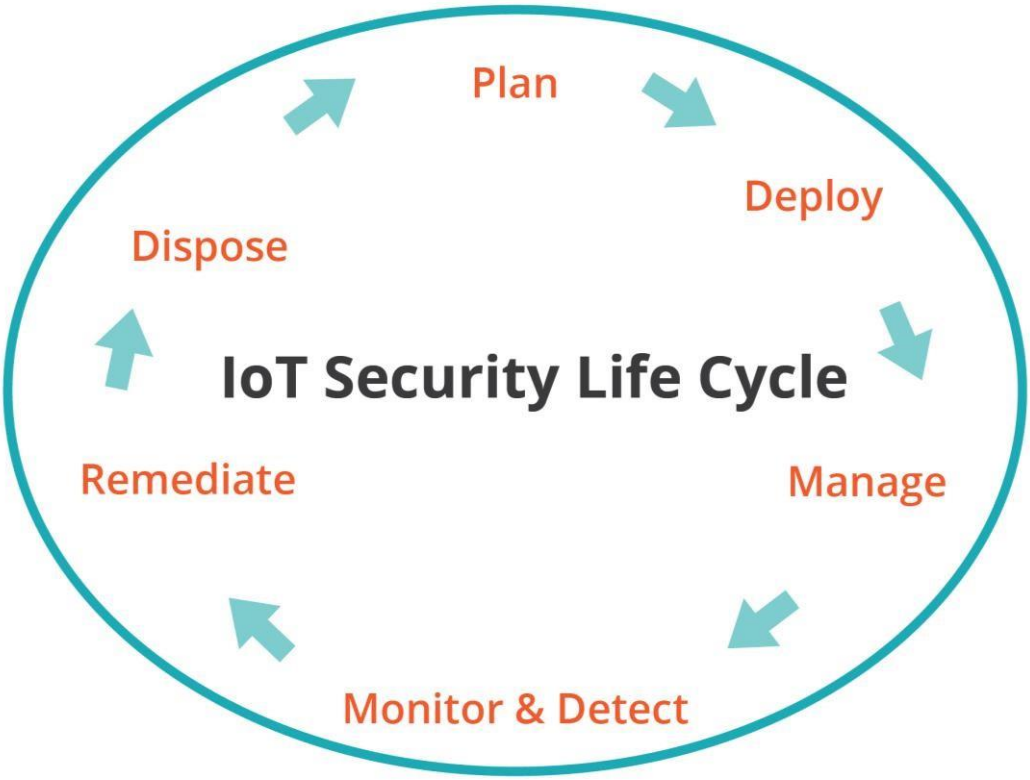
しっかりデザインした IoT の配備を考える上でデータ漏えい防止(DLP)は重要である。医療、機械制御、家電その他への配備のような例では大量の情報の収集と伝送が想定される。DLP は機微なデータが指定されたユーザベースまたはネットワークの外に拡散しないことを保証してくれる。DLP の検討は開発の初期段階で行われるべきで、また新しい IoT デバイスが企業のネットワークに導入される都度定期的に実施されるべきである。データ要素のタグ付けは適切な DLP のために重要な必要条件で、ポリシー適用点や XML ガードや一方向ダイオードやその他のデバイスで、機微なデータの伝送をフィルタし制御することを可能にする。

5.4.1.5. Aggregation Protection and Policies データ集積の保護とポリシー

大量の IoT デバイスは、そのこと自体によって様々なデータ分析システムにとって有用な巨大なデータを生成する。IoT セキュリティにとって重要なステップは、大量のデータが集積した時に、ユーザまたはシステムのプライバシーポリシーに確実に違反しないようにすることである。集積ポリシーはプライバシーの検討プロセスで実施され適切な管理が実装されるようにする必要がある。PPI（訳注：PII の誤りと思われる）データ、分割した PPI（訳注：PII の誤りと思われる）データ、集積防止、データの洗浄を検討してはいかがだろうか。

5.5. IoT デバイス用ライフサイクルのセキュリティ制御を定義する

IoT エッジデバイスのライフサイクルを制御するには、それらが認可され、安全であり、定期的に最新のファームウェアやソフトウェア、パッチなどが更新されていることを確実に管理し、監視されることが求められる。加えて、組織においては、ライフサイクルの最後に IoT 資産を確実に処分するための手順を文書化しておく必要がある。そこで、IoT デバイス用ライフサイクル管理アプローチを定義する。



5.5.1. 計画

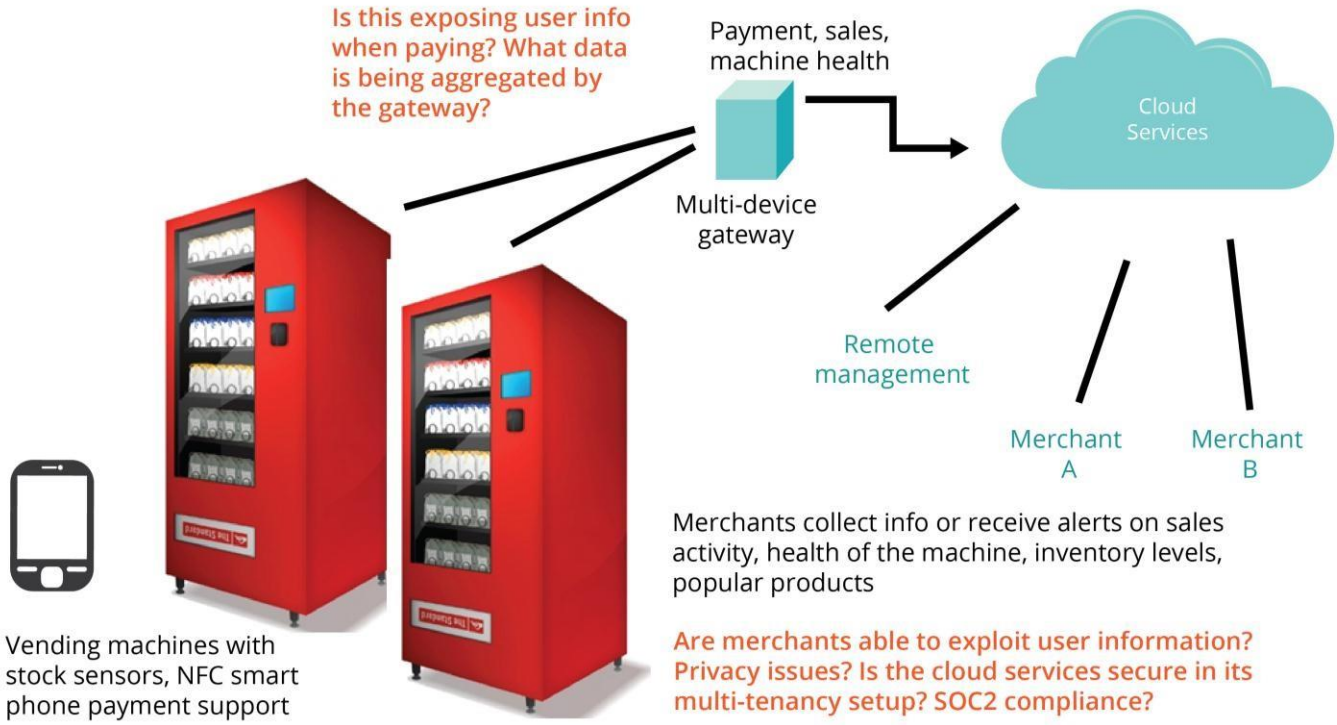
IoT の配備ごとに、セキュリティ管理や監視に必要なサポートインフラを検討する。特定の IoT を閉じた領域に区画するために、既存のセキュリティデバイスの最適なインターフェースを特定し、ネットワーク・アーキテクチャを更新する。

1	コミュニケーション計画	● どこにデバイスが置かれるか（企業内ネットワーク、その他） o デバイス内で強制されるもの；ネットワーク内の他のポリシー実施ポイントで強制されるもの o どの規約の下で、どのエンドポイントとどのエンティティが通信するのか ● 公開されたアクセス可能な IP アドレス（IPv4 の場合） ● IPv6 の 基準化と移行計画 o 近隣の検索 o 近隣への周知 o 拡張機能のサポート
2	物理的セキュリティ計画	● 配備環境を計画する；デバイスはどこにあり、どこに保管されているか？物理的セキュリティ（アクセス制御）はどのようになっているか？
3	論理的セキュリティ計画	● セキュリティ・ゾーン計画

4	監査行動基準の確立	● デバイスがどのような監査機能を有しているか？ ● デバイスに出入りするトラフィックを監視できる他の監査用捕捉デバイスで補完する必要があるか？ ● 正常運転時のデバイスの閾値は何か？閾値外になった場合、警告のトリガーとすべきものは何か？
5	認証/認可計画の確立	● デバイスの種類ごとの役割とサービスを文書化する ● セキュリティ関連の役割を区別する ● デバイスごとのアクセス制御マトリクスを確立する ● 必要に応じてデバイスの連携計画を確立する
6	デバイスおよび（/あるいは）デバイスがサポートしている情報の重要性を決定する	● 暗号化ツールに適用する、デバイス登録に必要な厳格さのレベルを決定する ● データおよびデバイス機能の保護のために必要な暗号化方式群を決定する
7	実装とブート処理の検証用テストを開発する	● インフラストラクチャが提供するセキュリティ機能への IoT デバイスの統合を検証する
8	エンタープライズ・アーキテクチャ文書の更新	● IoT 統合パターン
9	情報共有計画	● どのようなデータを共有できるのか？ ● どのようなデータが共有されるのか？ ● データのプライバシー管理策は何か？
10	プライバシー要件および管理策を確立する	● データのプライバシーが一緒になっている場合（例えば、薬箱のラベル） ● 必要な保護を維持することなく、データを任意に削減することが可能か？
11	安全要件および対応策の確立	● デバイスの多くは、認証/認可はサポートしていない。 ● 必要に応じ、リスクへの対応策を開発すること ● 利害関係者の安全上、機器の電子的不正利用の影響は何か？

スマートな自動販売機の IoT 実装が計画に関する考慮事項のよい事例を示している。

スマート自動販売機



5.5.2. 配備

1. IoT エッジデバイスの OS のための安全な設定
2. デバイス ID（アカウントと証明書）の確立；デバイスの記録（文書化）と棚卸し（資産管理）
3. 重要な機材と信頼関係の初期プロビジョニング
4. 運用上のセキュリティ検証と確認（V & V）
   a. 必要な監査データを取得しているか？
   b. アカウントは十分な管理下にあるか？
5. 異常想定テスト（オプション）
6. 必要に応じたゲートウェイの配備

5.5.3.管理

IoT デバイスの管理には、エッジデバイス自体、エッジデバイスにロードされたソフトウェアやファームウェア、ライセンス、デバイスの脆弱性対応のための日常的なパッチ更新の適用の管理が含まれる。IoT デバイスの管理は、企業内の一か所で全ての資産を管理していることもあれば、大きなプラットフォームに組み込まれた複数の IoT デバイスであることもある。それら管理ポイントはプラットフォーム自体に組み込まれており、エッジデバイスに向けた下り方向と管理サーバーに向けた上り方向の間でブリッジとして動作する場合が多い。暗号鍵、証明書あるいは事前に共有された秘密鍵は、各デバイスでも管理する必要がある。

5.5.3.1.資産管理

IoT エッジデバイスの種類は（低消費電力のセンサーから自動車内の ECU［エンジン制御ユニット］に至る）まで多様である。ほとんどの IoT エッジデバイスには、技術スタックに含まれる 1 つあるいは複数の層への更新が必要である。オペレーティング・システムはパッチ適用を要求され、ファームウェアは更新を要求され、専用アプリケーションもソフトウェア更新を要求される。IoT エッジデバイス上で稼動しているファームウェアやソフトウェアのバージョン履歴を保存しておくことは、資産管理の重要な側面であり、システム管理者が最小限の時間で適切なデバイスに必要な変更を素早く配備できるようになる。IoT デバイス上で稼動しているファームウェアやソフトウェアの変更を定期的に確認する手続きを定義し実施すること。基盤となる技術スタックへの更新を最終ベンダーに促されることがないようにすること。

変更が適正であり、改ざんされていないことを確認することは、従来のコンピューティング技術と同様に重要である。システム管理者は、全ての更新の信頼性と完全性を検証するためのプロセスの概要を説明し、取得し、保存し、IoT デバイスを更新するためのデバイス相互間におけるプロセスが確保されていることを確認する必要がある。

ファームウェアの更新を効率的に管理するため、IoT に適用できそうないくつかの規格がある。例えば、オープン・モバイル・アライアンス（OMA）のファームウェア・アップデート・マネージメント・オブジェクト（FUMO）やソフトウェア・コンポーネント・マネージメント・オブジェクト（SCOMO）は、エッジデバイスにファームウェアやソフトウェアの変更が出来るためスムーズに適合できそうである。今日、いくつかのベンダーは既にこれを行っており、OMA デバイス・マネージメント（OMA DM）ワーキンググループは、Bluetooth や ZigBee プロトコルをサポートするデバイスの管理を支援するゲートウェイ仕様（GwMO）を作成した。

SCOMO はデバイスのソフトウェア・コンポーネント一覧のようなデバイスからの情報を照会する機能も含んでいる。これはエッジデバイス上に不正なアプリケーションがインストールされていないことを確認する機能を備えているといえる。

当然ながら、IoT は単にデータを収集し送信するエッジデバイスについてだけではなく、データを移動させる転送経路やデータを処理するシステム、データを使用するシステムも含まれている。それらのアプリケーションやシステムのソフトウェア・バージョンも記録し、更新されることを確認すること。

IoT の規模が大きいため、IoT デバイスのハードウェア/ソフトウェア一覧が管理できることは組織にとって重要である。上記に加えて、ライセンス管理は重要である。自らの環境において、いくつのデバイスがあるか、すぐにわかるからである。資産を一覧できることは環境におけるデバイスの特定のハードウェア/ソフトウェアのバージョンを把握するためにも重要である。

IoT デバイスの特定のソフトウェア/ファームウェア・バージョンのセキュリティ・バグの事例を取り上げてみよう。- 適切な一覧がなければ「組織がリスクに晒されているかどうか、あるいは、組織への影響はないかどうか」について評価することはできない。別のケースとして、製品のファームウェアを更新する場合、それが適用できるかを判断しなければならず、更に製品の所有者は決定をくださなければならない。つまり。所有者と資産をマッピングすることは、その環境における資産一覧にとって、とても重要である。IoT 資産のライフサイクルを管理する責任は、その所有者が持つ必要がある。ツールやポリシーによる資産管理が助けとなる。

資産管理が適正に行われていない場合に起こりうる事としては、コンプライアンス問題（ライセンス/規制）、セキュリティ（安全であり続けるため、環境の中で何が必要か、知る必要がある – デバイス数/ファームウェアのバージョン/ライセンス状況/証明書/更新）につながる可能性がある。

5.5.3.2. 暗号鍵と証明書管理

たいていの場合、IoT デバイスは暗号鍵、証明書、あるいは事前に共有された秘密鍵を組合せて使用する。鍵と証明書を使用する場合、これらを生成し、配布し、一般的な管理を実施するセキュリティ対策の検討に注意を払うべきである。各デバイスの失効、セキュリティ侵害からのリカバリ、初期登録などは常に検討されるべきで、情報が保護されていることを前提に処理が進められる。

鍵は第三者がアクセスできるようにすべきではない。企業は、鍵の管理とライフサイクルを完全に制御すべきである。鍵と証明書のライフサイクルは、鍵データのセキュリティおよびユーザーやデバイスの鍵/証明書の結びつきを確かなものにする。ライフサイクルは、改変されたとみなされる証明書の処理や不要となった時の鍵データを破壊する処理も定義する。ライフサイクルの他の特徴は、定常的に企業全体に配備される鍵や証明書を使用する処理とともに、必要な時に鍵を回復する処理を含んでいる。

総合的なライフサイクルが定義されると、ベンダーが提供する安全な自動化機能の利点を説明できる機会を得る。証明書のプロビジョニングおよび再プロビジョニングは、合理化されたワークフローを提供する。しかし、新しい攻撃の機会を与えることを避けるために、プロセスを自動化することに伴う脅威を考慮することが重要である。

IoT 全体に配備された鍵と証明書の数が多くなると、それらを記録しておくことが難しくなる。そこでデバイスの証明書の有効期間を長くする必要性が出てくる。これは証明書の再提供の管理負荷を軽減するが、証明書が知らないうちに侵害され悪用される危険性が高まることにもなる。ネットワークと信頼関係がセグメント化されているため、組織が所有する IoT 内の全ての証明書と鍵の状況一覧を常に統合的に状況把握し続けることは可能ではない場合があるが、組織はできる限りこれを実施すべきである。

5.5.3.2.1. 証明書（鍵）の有効期限を制限しキーローテーションを適用する

一つの鍵の利用期間は、その鍵に関するリスクを判定するための重要な要素の一つである。暗号期間が無期限である鍵は、攻撃者が多くの時間をかけて総当り攻撃することを可能にするのと同時に、暗号解読を試みてデータを採取するための大いなる機会を与えている。鍵の暗号期間を選択する際、その鍵が保管される環境や使用される環境を理解しておくことが重要である。厳格なセキュリティ保護が提供された鍵は、保護されていないシステム（例：FIPS 140-2 で承認された暗号化モジュールを持たないスマートメーター）に保存される鍵よりも長い暗号期間で提供されることが多い。鍵の有効期間を短くすることで、鍵を不正に入手した第三者がその鍵を利用できる時間を短くするようにもできる。

エネルギー分野において、NISTIR は最大寿命が 10 年のようなユーティリティ用として提供されたデバイスの証明書に対して提供される鍵の有効期間を 3 年～6 年とするよう勧告している。この勧告の理由としては、特定の鍵と関連して暗号解読のために収集される材料の量を制限する必要性に基づいている。十分に強いアルゴリズムと鍵の長さが使用されることを仮定すると、定期的に鍵を更新することは、攻撃者の暗号解読の試みが有効であること制限することを確実にする。

証明書は、あるエンティティの公開鍵と秘密鍵の組合せを暗号化し紐付ける。鍵の組合せが更新されると、鍵の組合せと関連付けられた証明書も同様に更新する必要がある。鍵が暗号として十分に健全である場合に、単純に新しい証明書に簡単に結び付けるインスタンスがある。しかし、組織は定期的に更新され、攻撃者に対して防御していることを確実にするために、各デバイスの証明書の有効期限を制限する計画を検討すべきである。

IoT 製造業者から提供された証明書では有効期限設定されていない場合があるが、それは証明書に付すことができる信頼のレベルに関して疑問を生じさせるものであり、製造業者の CA がセキュリティ侵害を受けた場合の対策が必要であることを示している。

ある鍵の推奨される暗号期間は、その鍵の目的とタイプに依存する。鍵のタイプによる、具体的な推奨事項については、NIST SP 800-57 第 5.3.6 項を参照のこと。

5.5.3.2.2. 登録処理の定義と義務化

PKI 証明書を証明書利用者に提供するに際しての証明書を発行するための登録と承認は、PKI 実装のセキュリティを確保するうえで重要な要素である。PII（個人情報）あるいはその他の機密情報を処理するデバイスについては、データを保護するために適用されるその他の管理策とセキュリティ強度が同等である登録処理を適用するように注意を払うべきである。

5.5.3.2.3. セキュリティ侵害からのリカバリ計画を定義

すべての鍵管理の実装のために最も重要な側面の一つは、IoT エッジデバイスや、もっと深刻な場合は CA が、危険に晒されている場合に何をしなければならないかを、明確に理解していることである。エッジデバイスの暗号鍵や証明書が危険にさらされている場合、証明書失効の標準的な処理が行わなければならない。しかし同時に、セキュリティ侵害について調べてどのように鍵/証明書がセキュリティ侵害を受けたかを知り、修復対策が取られるようにし、事象の再発の可能性を制限するようにすべきである。

5.5.4. 監視と検知

- 脆弱性評価のようなセキュリティタスクや侵入テストのフォームを自動化すること
- IoT 脅威インテリジェンスの自動化のために、動的でリアルタイムで連続的なデバイス監視を開発すること

セキュリティの専門家は、常時多くのアプリケーションやデバイスを保護するために、通常過負荷状態にある。なぜならば、セキュリティ専門家一人当たり、50～60 名の開発者が潜在的な脆弱性をもつコードを開発している、という現実があるからである。したがって、手動による侵入テストという古い方法や四半期ごとのセキュリティ・レビューはだけでは十分ではない。手動で行っているセキュリティ・テストを、動的監視ツールを常時使用することで自動化する必要がある。

なおかつ、より人手をかけた侵入テストは、定期的に IoT のセキュリティ状態を効果的に評価するためにも必要である。IoT を考慮すると、露出した JTAG やシリアル・インターフェースを備えたデバイスの物理テストは自動化できない。精通したユーザーは、大規模配備された後に残されたハードウェア・インターフェースのデバッグをうまく利用することが出来る。このため、四半期毎に完全な侵入テスト活動を実施するようにする。

IoT は動的監視ツールを使ったビッグデータ分析を利用してリアルタイムに脅威を予測する機会も提供する。これは、組織がセキュリティ災害からより早く回復することを可能にする。動作や機能的操作を検査するために、各 IoT デバイスのヘルススキャンも推奨される。

理想的には 24 時間/365 日を基本として、IoT インフラ内のセキュリティ・イベントの監視も実施する必要がある。セキュリティに関連するデータの捕捉と、注目すべき事象や事象の組み合わせを検出するためのルールの確立を計画することは、エンジニアリング・ライフサイクルの早い段階で実施されるべきである。実装されているもののセキュリティ状態をほぼリアルタイムに監視する役割を持ったセキュリティ分析担当をもつことを検討すること。

IoT 実装の様々なソフトウェア・コンポーネントに関連する脆弱性、および IoT デバイス・タイプごとの最新の脅威について常時追跡することも重要である。特定の IoT 実装に対する様々な脅威を追跡し報告する役割を誰かに割り当てることを検討すること。

5.5.5.改善

新しい IoT システムを組み込むに際してインシデント対応計画を更新し、セキュリティが侵害された事象を取り扱う手続きを定めること。迅速に事象をエスカレーションさせるためにセキュリティ分析者を招集する計画を確立し、問題を調査し、改善するためのインシデント対応チームを出動させるための準備を整えること

5.5.5.1. 廃棄

数多くの IoT 実装に組み込まれている量からしてし、多くのエッジデバイスは定期的に交換されるであろう。機密情報を保持していたデバイスあるいは機密情報にアクセスできる主要なデバイスを安全に廃棄するポリシーと手順を確立することが重要である。機密情報を保持していたデバイスは、各デバイスから主要情報や証明書を消去することを含めて、安全に除去される必要がある。

5.6. IoT 導入のための認証と認可（権限付与）のフレームワークを定義し実装する

IoT においての認証のシナリオは様々である。IoT コンポーネントは相互に通信することがあり、その際、機器間（M2M:machine to machine）認証が必要になる。IoT コンポーネントはクラウドアプリケーションや、モバイルアプリケーションや、ウエブアプリケーション、さらには直接、人々とコミュニケーションをとることもある。IoT での認証と認可における、難題のひとつは、多くのデバイスが能力的に制約の多い条件下で動作していることである。つまり、使われている通信プロトコルでの認証機能が限定的だったり、たとえば証明書ベースの認証が利用できないというような、必要とされる認証機能がないといった問題だ。

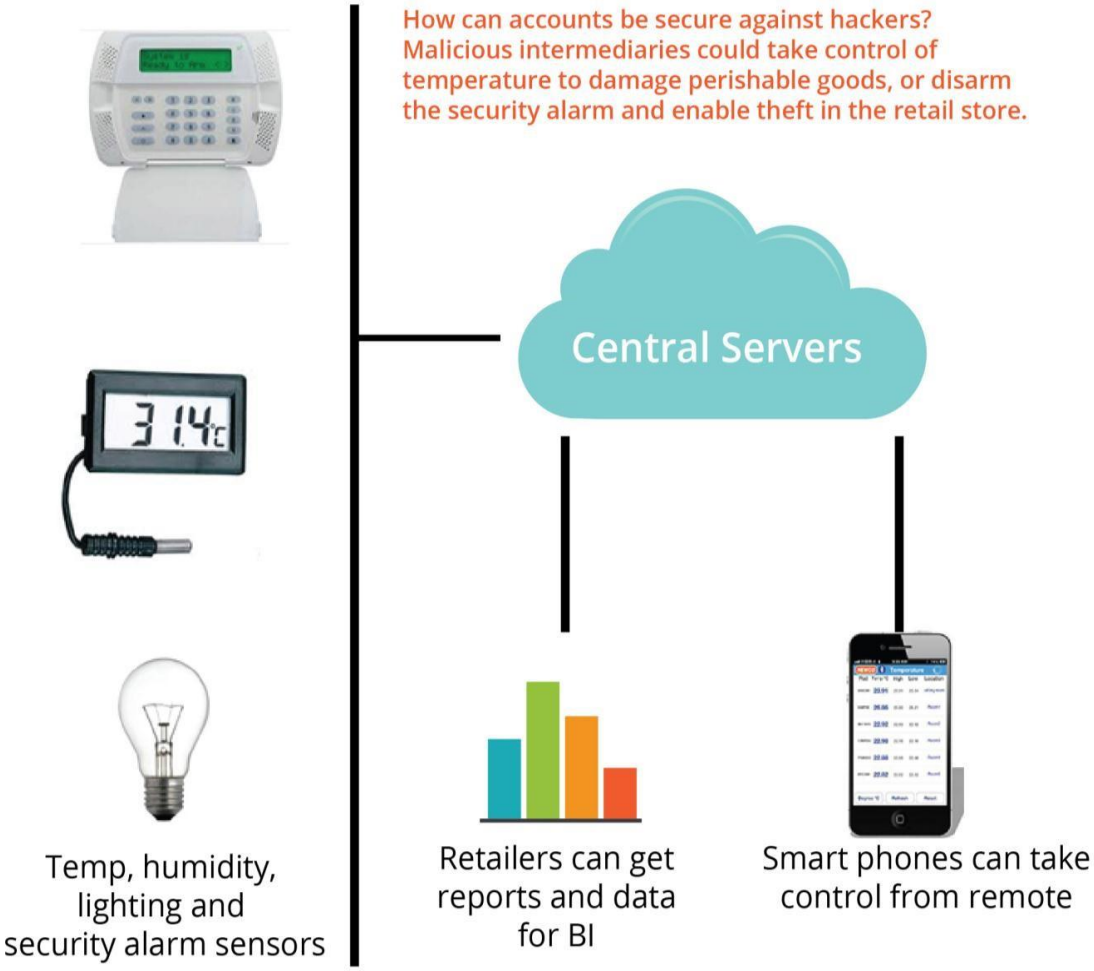
企業内での IoT コンポーネントの認証に関するユースケースは多種多様である。これら多くのユースケースは、抽象化した上で、以下のような IoT 認証に関する要求事項として一般化できる:

- IoT デバイスが他の IoT デバイスに認証されること
- IoT デバイスがゲートウエイもしくは制御装置に認証されること 、またはその逆
- ゲートウエイもしくは制御装置が（クラウドの）サービスに認証されること、またはその逆
- 様々なアプリケーションが（クラウド上の）サービスに認証されること
- IoT デバイスによるユーザ認証（たとえば、医療機器による医師の認証）
- IoT デバイスによる管理者認証（たとえば、道路に設置された機器による交通指令センター（の管理者）の認証）

小売業の例をとってみると、アカウントを侵害から守ることに関して、いくつかの疑問が浮かぶ。下図は、警備システムと環境制御システムが、複数の端末コンポーネントから情報を収集し、複数のモバイルデバイスと、その情報を共有している。[3]このシナリオにおいては、攻撃者が重要なシステムへのアクセスを獲得することで、物理的な損害を生じるというリスクを軽減するために、すべてのアカウントを十分に保護することが重要になる。

[3] 訳注：加えて、それらのデータを使用して環境制御などを行っていると考えられる

セキュリティアラームと環境センサー



今日、IoT の認証がどのように実装されているかを検証してみると、いくつかの選択肢があることがわかる。こうした選択肢には、以下のようなものが含まれる:

- プリシェアードキーもしくは共有秘密 [4]
- 電子証明書による認証
- トークンを使用した認証[5]

また、過去おいては、たとえば単に MAC アドレスのハッシュ値を認証に使用するといった脆弱な認証方法の実装が行われた例もある。こうした（弱い）アプローチは使い勝手はいいかもしれないが、セキュリティが要求される基盤においての利用は推奨できない。

共有秘密を使うことはできるが、大きな管理負荷が発生する可能性がある。もし、共有秘密を認証に使用するのであれば、NIST（米国標準技術局）が定義している HMAC（Hashed Message Authentication Code）に準拠し

[4] 共有パスワード等 を意味する
[5] ワンタイムパスワード等を意味する

た仕組みであることを確認する必要がある。HMAC においては暗号技術を用いてメッセージの内容とアイデンティティー（割り当てられた鍵）を結合する。HMAC では発信元の認証と同時に、メッセージの改ざん防止が可能である。HMAC スキーマの例として、HMAC-SHA-256 がある。

電子証明書による認証は、TLS や DTLS のようなプロトコルでサポートされる。証明書認証におけるひとつの課題は X.509 電子証明書のサイズの大きさに起因するものである。その代替としてとして機器間の通信認証やメモリサイズの制約が厳しいデバイスに特化したものがある。IEEE によって定められた 1609.3 証明書の構造は、車対車の通信に用いられる DSRC(Digital Short Range Communications)に使われる。この証明書の構造は、メモリ制限の厳しいデバイスに最適化され、X.509 よりも、かなりサイズが小さくなっている。こうしたデバイスや環境の制約に直面している開発者は、IEEE1609.3 証明書への移行の可能性を検討すべきだろう。

（X.509 や IEEE1609.3 などの）証明書の利用は、機器に対して発行する証明書を集中管理するための PKI（Public Key Infrastructure）を必要とすることにつながる。その必要性には、信頼できるデバイス登録や侵害からのリカバリといった重要な機能も含まれる。

トークンベースの認証スキーム、たとえば OATH2 や OpenID Connect による認証フェデレーションは、共有パスワードや証明書認証の代替として有用である上に、包括的なポリシー制御を IoT のアクセス要件に適用することができる。

選択される認証方式はデバイス（の能力）によって制約を受ける。共有秘密（パスワード）による認証は、証明書ベース認証の代替としてはあまり好ましくないと考えられている。共有秘密を使用することで、秘密を管理することの負担はデバイスの数の増加と共に膨大なものになる。一方で、証明書ベースの認証の採用は、証明書と鍵認証の確立といった非対称鍵暗号アルゴリズム処理（の負荷）に関する問題をもたらすことになる。

デバイス間通信においては、同列のデバイス間であれ、ゲートウエイもしくは集約装置とエッジデバイスの間であれ、サポートしているプロトコル自身に認証機能を持たせることがベストな選択であることも少なくない。たとえば、CoAP（Constrained Application Protocol）は 4 種類の動作モードを提供する。それぞれのモードは脅威レベルに必要な認証レベルを持っている。

- No Security　-- セキュリティは別のプロトコル層で実装する と想定
- preSharedKey　-- 通信を許可されたグループで対称暗号鍵を共有する
- rawPublicKey-- CoAP を実装するそれぞれのデバイスに一個の非対称鍵を使用する
- Certificate -- CoAP を実装した各デバイスに X.509 公開鍵証明書が配布される

CoAP において、”No Security”モードでは、セキュリティは他のプロトコル層に適用することが想定されている。preSharedKey モードでは、基本的な認証機能が提供されるが、鍵の安全保持や管理が難しくなることから、推奨はされない。preSharedKey モードはデバイスの通信ネットワーク内で他共有される単一の鍵にたよっている。このアプローチは小規模のデバイス群にとては十分だが、拡張性に欠ける。万一、鍵が漏えいしたような場合、全デバイスについて鍵を交換することは、時間がかかりかつ困難である。

CoAP を使用したデバイス間トランザクション認証における、よりよいアプローチは rawPublicKey または Certificate モードを使用することである。rawPublicKey モードは個々のデバイスにユニークな非対称鍵を配る

ため、一つの鍵が漏えいしても、すべてのデバイスの鍵を変更する必要がない。Certificate モードは、rawPublicKey モードと似ているが、さらにデバイスのセグメントを信頼する手段（信頼できる存在にある CA 発行者をベースとした）や強力な鍵の無効化手続を提供している。）デバイスに公開鍵基盤(PKI)を適用する場合には基本的にこのモードを用いるべきである。

認証という切り口での IoT プロトコルに関する調査結果を以下に示す:

プロトコル	m2m 認証オプション	分析
MQTT	ユーザ名とパスワード	MQTT はユーザ名とパスワードを伝送できるが、パスワードの長さは 12 文字までに制限される。ユーザ名とパスワードは平文で転送されるため、MQTT の利用においては、TLS が必須となる。
CoAP	事前共有鍵 公開鍵 電子証明書	CoAP はデバイス間通信において複数の認証オプションをサポートする。データグラム TLS（DTLS[6]）と組み合わせることで、より高いセキュリティを確保できる。
XMPP	複数の認証方式（プロトコル）をサポートする	XMPP は SASL[7](Simple Authentication and Security Layer –RFC4422)を介して、様々な認証方式をサポートする。一方向の匿名認証や双方向の暗号化パスワードを使った相互認証、電子証明書、SASL の抽象化レイヤで実装可能なその他の方法がある
DDS	RSA や DSA アルゴリズムを使用した X.509 証明書（PKI） トークンを使用した認証	Object Management Group による DDS[8](Data Distribution Standard)のセキュリティ仕様では、エンドポイント認証に加え、その後実施されるメッセージデータの（HMAC[9]等を使用した）発信元認証のための鍵交換を提供する。電子証明書や、様々なタイプの ID・認可トークンがサポートされている。
Thread	（ベータバージョン、まだリリースされていない）	スマートデバイスネットワーキング用の IPv6 ベースのプロトコルである Thread では、他のプロトコルで使われているセキュリティオプションを利用し、また改良するものと見られている。
Zigbee (802.15.4)	事前共有鍵	Zigbee は、マスター鍵（オプション）またはネットワーク鍵（必須）または、アプリケーション鍵を使ったネットワークレベル認証とアプリケーションレベル認証の両方を提供する。[RBJ1]
Bluetooth	共有鍵	Bluetooth は標準ペアリング及び単純ペアリングのという二種類のオプションによる認証サービスを提供する。標準ペアリング方式は自動化されている。単純ペアリングでは、人が介在して（単純な Diffie-Hellman 交換の後で）二つのデバイス間で交換された鍵が同じハッシュを示すことを検証する。Bluetooth では、一方向の認証と相互認証の両方を提供する。 Bluetooth のセキュアで簡単なペアリング方式では、デバイス間認証のために、「とりあえず動く」、「パスキー入力でのペアリング」「出荷時設定で動作する」といった選択肢が可能である
Bluetooth-LE	データ暗号化なし CSRK[10]による認証 IRK[11]によるデバイスの識別とプライバシー確保	Bluetooth-LE は、Bluetooth の世界に二要素認証を提供する。LE セキュアコネクションペアリングモデルでは、デバイスの能力に応じて数種類のアソシエーションモデルを利用できる。また、鍵交換には楕円曲線 Diffie-Helman 方式が使用される
HTTP/REST	ベーシック認証 （平文または TLS） OAUTH2	HTTP/REST は、一般に認証と機密性維持のために TLS プロトコルのサポートが必要である。ベーシック認証（識別情報が平文で渡される）は TLS のもとで利用できるものの、これは推奨される方法ではない。かわりに、OAUTH2 のような、トークンベースの認証方式の利用を試みること。

[6] 処理能力の低いデバイスなどで利用できるように処理負荷を減らした TLS プロトコル
[7] Simple Authentication and Security Layer(RFC4422)
[8] DDS : The Object Management Group Data Distribution Standard
[9] ハッシュ関数を使用したメッセージ認証コード
[10] Connection Signature Resolving Key
[11] Identity Resolving Key

IoT の導入において適切な認証方式を選ぶにあたって、以下の質問を参考にすることができる:

1	その実装において、デバイス相互の通信は必要か	必要であれば、デバイス間通信プロトコル自身が（デバイスの）認証をサポートしているか確認する
2	IoT デバイスは認証サービスを提供する通信プロトコルのいずれかをサポートしているか	サポートしていなければ、TLS や DTLS など上位のプロトコル層での認証を検討する
3	使用している IoT デバイスにメモリまたは処理能力の制約はあるか	制約がある場合、（X.509 ではなく）IEEE1609.3 証明書をサポートするために、ベンダとの協力を検討する
4	誰がデバイスを管理するか。遠隔管理は必要か。	まず実装をきちんと計画すること。認証とアクセスコントロールに関するマトリクス表を作り、エッジデバイスがサポートしている最も強力な認証方式を選択すること
5	IoT デバイスは、SNMP や SSH などのネットワーク経由の管理機能を提供するか	設置前に必ず正式な管理サービス以外から接続できないように接続を制限しておくこと。デバイスのネットワーク経由の遠隔管理に関するポリシーや手順を整備すること。
6	IoT デバイスが RESTful なインターフェイス（API）を実装しているか	エッジデバイスに対して、OAUTH2 のような、トークンベースの認証方式の利用を検討する
7	IoT デバイスは、クラウドにあるサービスに直接接続されるか	認証の設計に際して、クラウドサービスへのデバイスおよびアプリケーション認証をサポートする API 鍵を確実に含めるようにすること。

5.6.1. API 及び API 鍵に関する議論

API のセキュリティは、IoT セキュリティにおいて重要なパートである。IoT 事業者は、オープンな API を製品に組み込むことで、様々な用途や可能性を切り開きつつある。こうした API についての動きは、IoT 業界におけるエコシステムを加速させることとなり、IoT ベンダにとっては自社の環境のセキュリティを第一に考えることが必須となる。もうひとつの懸念は、グローバルにデバイスが接続され相互に通信できるる環境において、デバイスベンダによる（クラウドサービスや他社デバイスの）API の不正利用を阻止するという点である。我々は、個々のデバイスに閉じた環境とグローバルに接続された（オープンな）環境の両方について、その要求に見合うセキュリティモデルを開発する必要がある。

5.6.2.アイデンティティとアクセス管理

IAM に加え、特権ユーザ管理システムを導入することで、管理者や管理コンソール、アプリケーションのの動作や相互間のやり取り活動を追跡する。とりわけ大規模な IoT 導入において、これは有益であり、資格情報の管理ポリシー策定や、利用の都度パスワード変更を義務付けること、資格情報の発行や削除を行わせること、活動記録（フォレンジックのためのキー入力の記録など）の作成を必須とすること、に役立つものである。

一般消費者のアイデンティティ管理、とりわけ小売業界や運輸業界における管理には、ポリシーベースおよび同意に基づいた集中管理システム、という考え方があり、以下のような点について消費者が同意するかどうかの意思決定をサポートしている:

- どの属性や情報を開示してよいのか
- 表示、印字する際、どの情報をマスクする必要があるのか
- どの情報を第三者による分析やマーケティング目的で使用できるか
- その他の要望事項

これらは、法規制の遵守と深い関連があるが、こうした要件を組織のセキュリティポリシーに取り込む事で、より強固なセキュリティの枠組みを作ることができる。

IoT デバイスを含むすべてのサービスを集中管理するポリシーベースの IAM を持つことは、個々のデバイスとそれに関連するサービスごとに分散した IAM を持つことに比べて、管理が容易になる。全体で統一されたポリシーに基づいて全体のシステムを強化し堅牢化することは、個々のサービスごとの個別の認証、認可を実装するよりも一貫性を確保出来る。

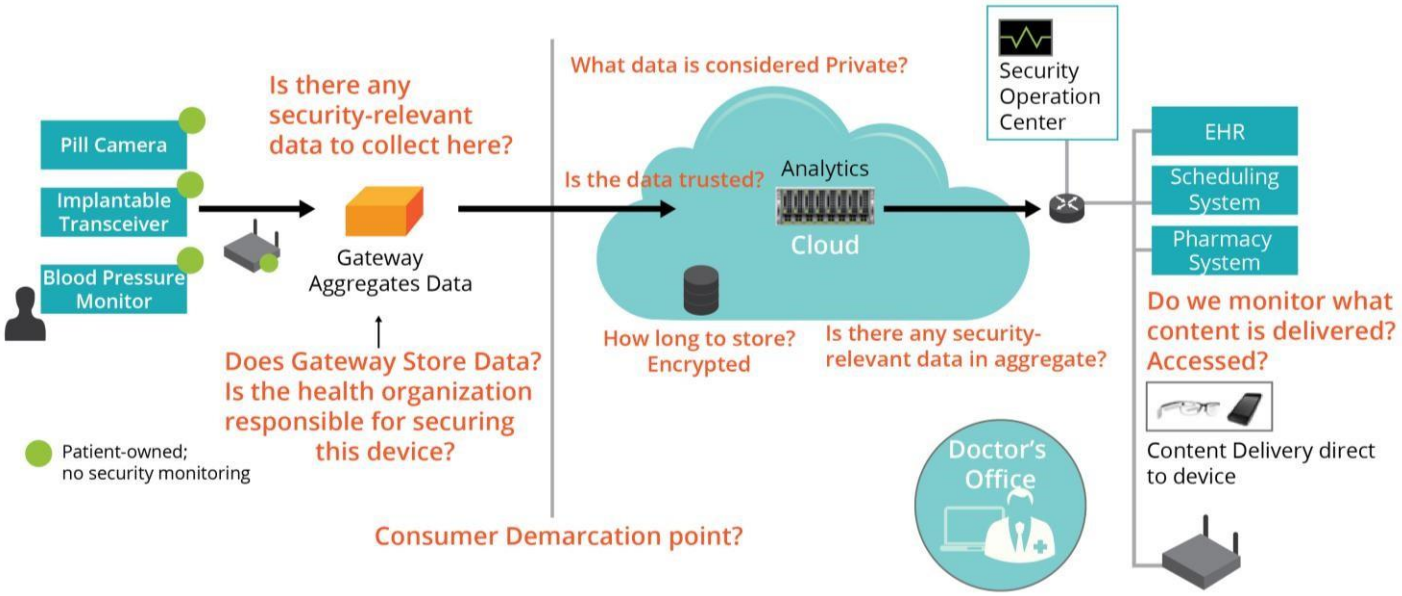
5.7. IoT エコシステムにおけるロギングと監査のフレームワークを定義する

現在の IoT デバイスは、一般に SIEM との連携機能を有さない。また、SIEM システムもまた、大量かつ広範囲に設置された IoT デバイスのモニタリングに十分であるかどうか定かではない。多くの場合、IoT デバイスは、API（アプリケーション・プログラム・インターフェイス）経由でのデータ取得[12]をサポートしておらず、またいくつかのデバイスは、IoT を基盤としたデータ解析に不可欠なデータを提供するが、外部の組織に所有されている場合もある。全体を包含するロギングのアーキテクチャを定義する上での、別の制約として、（ログの）データを無線で送信することのコスト負担も考えられる。これは多くの場合、実用に耐えないレベルのバッテリー消耗をもたらすことになる。

IoT の監査とロギングフレームワークの計画を行うにあたって、参考利用事例を検証することが役立つ。下の図は、遠隔の患者モニタリングシステムの例である。

[12] 訳注：主としてログデータの取得を意味する

遠隔での患者モニタリング

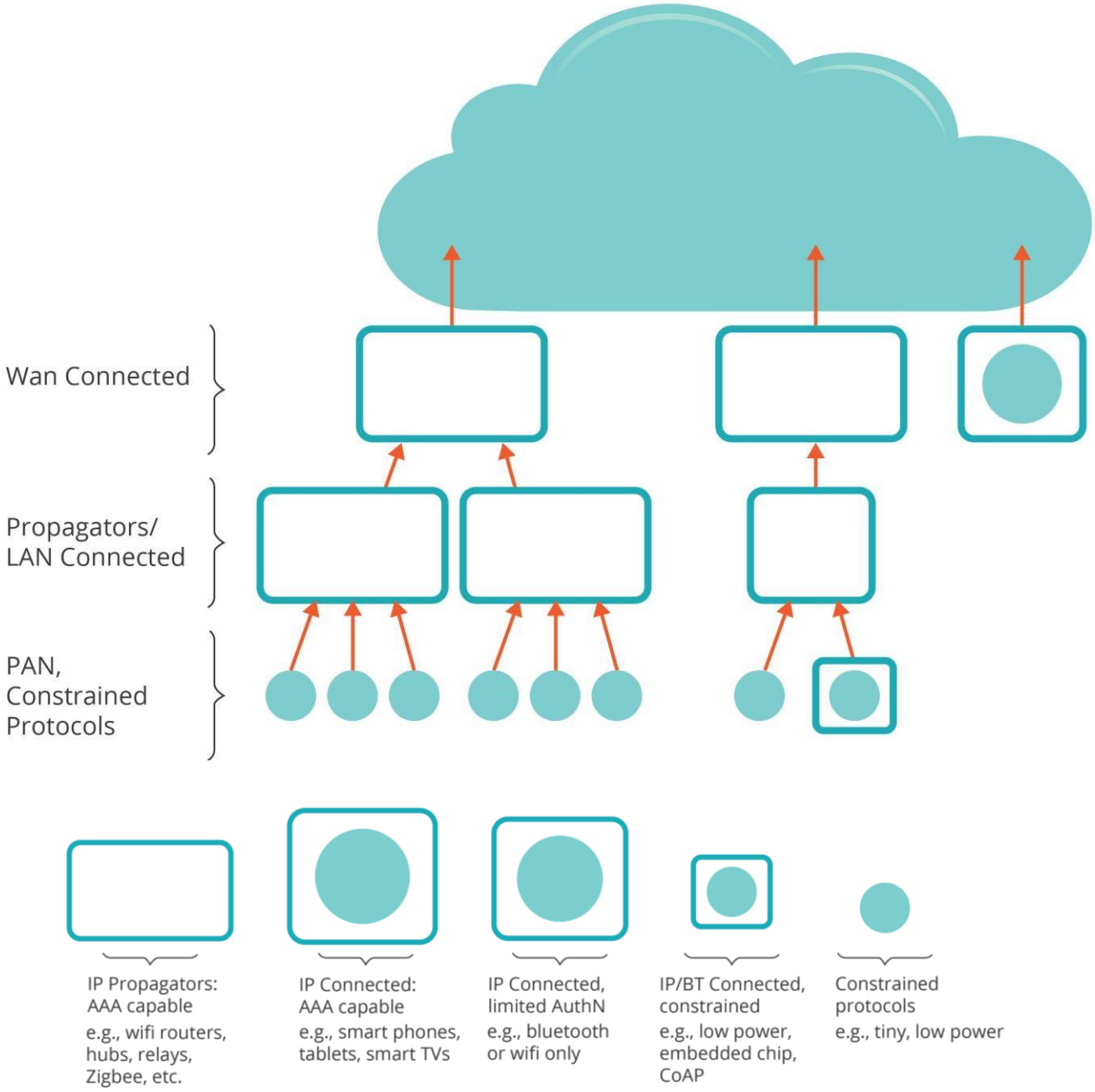


これを見ると、IoT エコシステム内のどのコンポーネントが実際に監査用データを提供でき、どのコンポーネントが、運用上のデータの流れのから異常な動作を検出できるように掘り下げるべきなのかを理解することが重要であることがわかる。この例でいうならば、どのコンポーネントがコンシューマ（患者）側に帰属しているか考えることが、（たとえばログイン失敗のような）適切なデータを取得でき分析することに役立つ。また、監査ログに、機微な（プライバシーに関する）データが含まれないか、（暗号化など）十分な保護がなされていない場合には、確認することも重要である。

5.7.1.ゲートウエイとアグリゲータの利用

現在の IoT デバイスにおける制約を考えるならば、IoT システムの状況を常に知っておくためには、独自のアプローチが必要である。IoT の設置においては、単独型のセンサーの場合もあれば、複数のセンサーや他のデバイスを統合したものの場合もある。後者の場合は、エンドポイントのログをアグリゲータ（集約装置）もしくは伝送装置に送る多層構造をとるのが賢明だろう。そうすれば、これらの伝送装置は各デバイスが使用する異なるプロトコルを翻訳し、分析のために、より高度な情報統合を行うことができる。

Gateways and Aggregators



この階層化されたアーキテクチャでは、非常に制約の大きいデバイスをもエッジに置くことができる。こうしたデバイスは、最小限の機能しか持たず、ある種の無線プロトコルで接続されることが多い。これらのデバイスは、組織の LAN に接続された、より能力の高いデバイスに接続されることで、収集された情報を送信するために他のノードに委ねることができる。このアーキテクチャでは、同様に組織内の様々な固有のネットワークセグメントに分散したデバイスからセキュリティ情報を集めることができる。IoT の一つの特色は、多くの異なるタイプのデバイスが、多くの論理的、もしくは地理的な領域にまたがって存在することである。こうしたデバイスすべてからデータを収集するためには、監査ログデータを記録、伝送するための標準的なデータフォーマットが必要である。

データ収集、処理するデバイスの多さに起因する情報過多は IoT におけるもう一つの懸念点である。セキュリティに関連する必要なデータのみを収集するように監査データ収集をチューニングすることは、過大な情報によって誤報を誘発することや十分に情報を処理できないことで真の脅威を見逃すリスクを最小化するために重要である。

より面倒な問題として、IoT のクラウドへの論理的拡張がある。IoT は物理的、論理的な形の両方で存在しうるので、データの収集はその両方から行う必要がある。

IoT デバイスが収集、通信する業務用のデータと、セキュリティ状況把握のためのセキュリティ監査データを区別して考えることは重要である。業務用データ、たとえば温度センサーから送られる水温のデータのようなものは、必ずしもセキュリティには関係がないので、統合、分析のために上流に送る必要はない。

将来的には、こうしたインラインのデータ（業務用 IoT データ）とセキュリティ監査データの関連性を検討する動きが顕著になるだろう。データ解析システムをチューニングして潜在的なセキュリティイベントを特定し、SIEM に対してフィルタされた出力を供給することは、セキュリティ上大きな価値を生むだろう。

5.7.2. ロギングデータ

一般に、インシデントが発生したか発生しそうかを示すデータをロギングすることは重要である。可能な限り、最低限、以下のデータ要素は記録されるべきである。

5.7.2.1.記録すべきイベント

- 権限昇格の失敗
- デバイスへのログイン失敗
- サービス事業者（クラウド）へのログイン失敗
- デバイス間認証の失敗
- データベースアクセスの失敗
- ポリシー変更
- 特権の使用
- アカウントの作成
- アカウントの変更
- トンネリング接続の失敗
- 内部状態
- 電源オン／オフ
- 特定のファイルシステムにおける完全性の変更

5.7.2.2. ログに記録すべきメタデータ

- （イベント）開始時刻
- （イベント）終了時刻
- （実行した）ユーザ
- 相手デバイスの ID
- 宛先デバイスの MAC アドレス
- 宛先デバイスの IP アドレス
- 宛先デバイスの IPv6 アドレス
- 宛先デバイスのホスト名
- トランスポートプロトコル
- データリンクプロトコル

5.7.2.3. ログの取得場所

ログ取得は、一部の機能が限定されたデバイスで直接ログ収集やその定期的な転送ができないとしても、可能な限りエッジデバイスに近い場所で行うべきである。このような場合には、Wi-Fi その他のプロトコルのルータ、ゲートウエイ、標準的なネットワークセキュリティデバイスのような IP 伝送装置でのデータ収集を通じて状況監視ができているかどうか、評価されるべきである。

5.7.3. セキュリティログの伝送

エッジデバイスやアグリゲータからのログは伝送時に暗号化と認証が行われること。

5.7.4. セキュリティ上の考察

IoT デバイスからのログ転送で重要な点のひとつが、機微なもしくは個人特定情報を暗号化すべき点である。これには、監査データのエッジデバイスや伝送装置での保存や、監査・ロギング用コンポーネント間の転送のための暗号化が含まれる。

6. 今後の取り組み

IoT には業界全体のイノベーションや採用を促進する無限の可能性がある。これらの機会とともに新しい脅威ベクトルも現れる。これらのセキュリティリスクを軽減する取り組みは IoT に特化した標準や技術の開発の中でイノベーションを生み出すだろう。

6.1. 標準

不幸にも IoT はすべての側面において標準が欠如している。これは IoT 機能を提供する多様な通信プロトコル、メッセージバス、プロセッサ、そしてオペレーティングシステムを調べればわかる。今日の組織は独自のユースケースをサポートするパッケージ IoT システムを購入できず、自身のシステムを開発しなければならない。この複雑性は IoT システムの誤構成や脆弱性を予示する。IoT デバイスにセキュリティ保証を与える新標準は IoT を実装する上で、上記の脅威やリスクに対応するのに役立つと期待される。今日、このようなスキーム(例えばコモンクライテリア）は主にハイエンドシステムでのみ利用されている。

6.2. IoT セキュリティ状況を把握する仕組み

産業界は、IoT が提供し分析する操作データのストリームから、適切なセキュリティデータを確認する方法に取り組まなければならない。これによりセンサーが提供する操作データストリームの例外の振る舞いを特定することや、振舞パターンの変化や通常外のインプットに基づいて、ある単一のセンサーかセンサーの小さなグループがセキュリティ侵害を受けたかどうかの情報を示すことが可能になる。データ分析プラットフォームと SIEM の間をつなぐ標準化された API の確立は、組織における IoT 実装の全体的なセキュリティ状態を把握することを可能にする。データ分析システムをチューニングしてセキュリティイベントの可能性を特定することや、そのようにフィルタされたアウトプットを SIEM に提供することはセキュリティ上の価値を著しく高める。

6.3.情報共有

IoT は一般に、デバイスの規模が大きくかつその技術が新しいために、一連のゼロデイ攻撃が起き、IoT の実装で見つかった弱点を悪用されるだろう。新しいエクスプロイトに晒される期間を減らすために、組織は IoT の情報共有・分析センターに参加することを考えなければならない。これは組織間の協力関係を構成し、共通の関心を持つ、あるいは同種の組織間で統計データや脅威に関する情報を共有することを可能にするだろう。

6.4. SDP と IoT

IoT は多くのケースでデータ伝送をクラウドに依存する一方、ペリメタ(境界線）セキュリティの伝統的な考えは時代遅れとなりつつある。SDP (Software Defined Perimeter)と IoT を結び付ける研究は、IoT への攻撃に対する防御として、階層的セキュリティとネットワーク防御を実現する上で、大きな利益をもたらすだろう。

6.5. IoT 環境のプライバシー

IoT には検討しなければならないプライバシーに関する懸念が多くある。一つの重要な懸念は消費者が知らないセンサーからデータが収集される問題だ。これらの場合、個人は知らずに組織や他の個人に監視されたり追跡されたりする。このシナリオでは多くの問題がある。一つは、追跡された人はいかなる賠償請求権を有するか、という問題であり、もう一つは、第三者の組織は、その収集した情報が明確な同意無しで集めたものでないことを保証するためにどのような責任を負うのかという問題である。

最後に、我々にとって重要なことは、オフプライバシー要件の組合せ（通知、認識、選択、同意、アクセス、法的強制権など）のうちどれが技術的なコントロールで実現でき、どれが IoT アーキテクチャの範囲では対応されないのかを明らかにすることである。同様に、収集されたデータのうち、属性に関するどの要素が、捕捉され伝送され、IoT システム全体の中でのデータフローのライフサイクルを通じて保持されるかの問題がある。例えば、もし誰ががデータ収集時点でその使用に同意した場合、その判断は、他の IoT プレイヤーによるデータの共有、伝送、分析にどこまで付随していくことになるのか？　そのデータがオリジナルの同意に基づいて処理されていることを確実にするために、データにタグをつけ、エコシステムを構成するパートナーとの間でそのことを伝達していくことは可能か？これは、匿名の要素と限定して収集されたデータが、事後に再識別される問題も含む。

Appendix A: 参考資料

ITU-T Y.2060 Overview of the Internet of Things @ http://www.itu.int/rec/T-REC-Y.2060-201206-I

State of the Market, The Internet of Things in 2015, Verizon @ http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-thingshttp://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf2015_en_xg.pdf

Industrial Internet of Things Positioning Paper, Accenture @ http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Thingshttp://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.PDFPositioning-Paper-Report-2015.PDF

IDC Futurescape for Internet of Things, December 2014 @ https://www.idc.com/getdoc.jsp?containerId=prUS25291514

Mitre Common Vulnerabilities and Exposures @ https://cve.mitre.org/

SOHO Wireless Router (In)Security: Tripwire Vulnerability and Exposure Research Team (VERT) Report, 2014 @ http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/

Dan Geer Security of Things Forum, May 2014 @ https://securityledger.com/2014/05/dan-geer-keynote-securityhttps://securityledger.com/2014/05/dan-geer-keynote-security-of-things-forum/of-things-forum/

Symantec Corporation Internet Security Threat Report 2014 Volume 19 @ http://www.itu.int/en/ITUhttp://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdfD/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show Las Vegas, Nevada January 6, 2015 @ https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf

Software Defined Perimeter (SDP) Specification Document v1.0 @ https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf

Privacy and Data Protection Impact Assessment Framework for RFID Applications 12 January 2011 @ http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

Article 29 Data Protection Working Party: Opinion 8/2014 on the on Recent Developments on the Internet of Things @ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionhttp://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdfrecommendation/files/2014/wp223_en.pdf

Threat Modeling: Designing for Security by Adam Shostack @ http://threatmodelingbook.com/index.html

Microsoft Developer Network: The STRIDE Threat Model @ https://msdn.microsoft.com/enhttps://msdn.microsoft.com/en-US/library/ee823878(v=cs.20).aspxUS/library/ee823878(v=cs.20).aspx

Microsoft Developer Network: Threat Modeling — DREAD @ https://msdn.microsoft.com/enhttps://msdn.microsoft.com/en-us/library/ff648644.aspxus/library/ff648644.aspx

MITRE's Common Vulnerabilities and Exposures @ https://cve.mitre.org/index.html

OWASP's Top 10 Threats for Internet of Things @ https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

