IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach

Release 1

Contents

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document,

https://iotsecurityfoundation.org.

can be seen on the public website at:

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organization which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

All product names are trademarks, registered trademarks, or service marks of their respective owners.

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document

John Moor, IoT Security Foundation
Richard Marshall, Xitex Ltd
Stacie Walsh, Oxford Information Labs

Peer reviewers:
Chris Shire, Infineon Technologies Ltd
Jeff Day, BT
Paul Dorey, IoTSF Chairman
Robert Dobson, Device Authority Ltd
Steve Babbage, Vodafone
Plus others – you know who you are!

1 Introduction

1.1 Executive Summary

The opportunities and benefits that exist for businesses to use IoT-class products and systems are many and varied. These may include improving the customer and employee experience, streamlining operations, improving productivity or even creating new avenues of business. With a wide range of procurement, installation, configuration and operating options, a common challenge is how to manage and maintain a complex system. This is especially important when it comes to security as the benefits of IoT could be overshadowed by the risk of adoption.

企業がIoT-classの製品やシステムを用いるとき、その機会と利益は多種多様なものとなる。 そこに含まれるものとしては、顧客と従業員のエクスペリエンスの向上や、運用の合理化、生産性の向上に加えて、新しいビジネス開拓などが挙げられる。 調達／設置／構成／運用に幅広い選択肢があるが、どのようにして複雑なシステムを管理／保守するかという点が、共通の課題として浮かび上がる。IoTを採用するメリットが、そのリスクにより希釈される可能性もあるため、セキュリティは極めて重要になっていく。

The IoT Security Foundation is publishing a series of architecture proposal documents with the following intentions:

IoT Security Foundationは、次の目的を達成するために、アーキテクチャを提案する一連のドキュメントを公開している。

- Reduce/manage complexity of IoT systems by simplifying implementation options
- Demonstrate what a good security regime looks like, by example
- Explain the benefits of a hub-based approach including achieving security goals, maintaining system hygiene and resilience, managing extensions and life-cycle provisioning

- 実装におけるオプションを簡素化することで、IoTシステムの複雑さを軽減／管理する
- 例を挙げることで、優れたセキュリティの形態を示す
- Hub_baseアプローチの利点を説明する。そこには、セキュリティ目標の達成や、システムの健康状態と回復力の維持、拡張機能の管理、ライフサイクル・プロビジョニングなどが含まれる

A hub-based architecture may not be a single device/interface solution, but a collection of security and trust tools. For small enterprises, the architecture may comprise a single device; for larger enterprises, it will likely consist of a number of hubs, both for scalability and redundancy. Related devices and solutions that may act as the hub in this architecture include a router, network management and security tools such as a firewall or gateway, network access controls, a protocol bridge or any other device that naturally lends itself to a management role within a network. In practice, a hub architecture provides selected points for IoT device and network management that can make use of existing infrastructure, as well as provide flexible bespoke solutions for individual IoT deployments.

Hub_baseアーキテクチャは、単一のデバイス／インターフェイスによるソリューションではなく、セキュリティおよびトラスト・ツールの集合体だと考えられる。 中小企業においては、単一のデバイスによりアーキテクチャが構成される場合がある。大企業においては、スケーラビリティと冗長性を担保するために、、多数のハブによりアーキテクチャが構成される可能性がある。このアーキテクチャのハブとして機能すると考えられるデバイスとソリューションには、ルーターおよび、ネットワーク管理、セキュリティ・ツールなどが含まれる。それらは、ファイアウォール、ゲートウェイ、ネットワーク・アクセス制御、プロトコル・ブリッジなどの、ネットワークを管理するための機能を提供する。実際のところ、既存のインフラストラクチャを活用できる、IoTデバイスとネットワーク管理のための選択されたポイントを、なんらかのハブ・アーキテクチャが提供している。それに加えて、それぞれのIoTデプロイメントのための、柔軟なオーダーメイド・ソリューションも提供される。

This document is intended to illustrate a solution for enterprise environments where businesses are looking for operational and productivity benefits of using IoT. It is intended for chief officers or managers – such as those tasked with overseeing IoT adoption, information security, or digital transformation – as well as staff with responsibilities for architecting, designing, planning, procuring and operating an IoT-class system – i.e. system architects, technical managers and systems integrators. It may also be of use to companies designing smart hubs as 'the Hub' is a key element of the architecture. Security is not static, it requires a series of on-going processes that need to be managed over the combined life-cycles of system elements including services, devices and networks.

このドキュメントの目的は、IoTの活用により運用上／生産性上のメリットを求めるエンタープライズのための、ソリューションを説明することにある。想定する読者は、IoTの採用や、情報セキュリティ、デジタルトランス・フォーメーションを任務とする、最高責任者またはマネージャーである。つまり、IoT_Classシステムの設計／設計／計画／調達／運用を担当するスタッフであり、役職はシステム・アーキテクト／テクニカル・マネージャー／システム・インテグレーターになるだろう。ここで言うHubは、アーキテクチャの重要な要素であるため、スマートハブを設計する企業にとっても、役立つものになるだろう。セキュリティは静的なものではない。そして、サービス／デバイス／ネットワークなどのシステム要素のライフサイクルを組み合わせて管理する、進行中のプロセスのつながりを必要とする。

The architecture described by this document supports a layered approach to the security challenge and lifecycle management tools in the Enterprise IoT deployment. It presents a relatively user-friendly IoT management solution that supports key principles of security assurance and good practice including network management, connecting devices securely, software maintenance and end-of-life considerations. As a result, it may also support a number of specific compliance requirements or best practice standards. For example, a hub-based architecture can help mitigate risk associated with cyber security and data protection regulations such as the European General Data Protection Regulation (GDPR) [ref 13] and Network and Information Systems (NIS) Directive [ref 14] or support adoption of the USA's Cybersecurity Information Sharing Act (CISA) [ref 15].

このドキュメントで説明するアーキテクチャは、エンタープライズIoTデプロイメントの、セキュリティ課題とライフサイクル管理ツールに対する、階層化されたアプローチをサポートする。そこで提供されるのは、セキュリティ保証の主要な原則と、適切なプラクティスをサポートする、比較的ユーザーフレンドリーなIoT管理ソリューションであり、ネットワーク管理／デバイスの安全な接続／ソフトウェア・メンテナンス／利用の終了に対する考慮などを取り込むものとなる。その結果として、多様なコンプライアンス要件やベストプラクティス標準も、サポートすることになるだろう。たとえば、ハブベースのアーキテクチャは、European General Data Protection Regulation (GDPR) [ref 13] や、Network and Information Systems (NIS) Directive [ref 14]で定義される、サイバー・セキュリティおよびデータ保護規則に関連するリスク軽減にも役立つ。そして、USA's Cybersecurity Information Sharing Act (CISA) [ref 15] の適用をサポートする。

Whilst perfect security is likely to remain elusive, this architecture is considered to be a good approach to support the management of common security goals of confidentiality, integrity and availability. Interoperability between IoT devices is a key aspect of hub architectures, like the one described here, and assists with security management across the IoT ecosystem. While this document does not specifically address the issues related to interoperability, it is worth highlighting the work that should be done in this area to support IoT security and ease of adoption.

完璧なセキュリティといっても、捉えどころが無いだろうが、このアーキテクチャは、機密性／完全性／可用性という、一般的なセキュリティ指標を管理するための、優れたアプローチであると考えられる。IoTデバイス間の相互運用性は、ここで説明するハブ・アーキテクチャの重要な側面であり、IoTエコシステム全体のセキュリティ管理を支援する。このドキュメントでは、相互運用性に関連する問題を具体的に取り上げていないが、IoTセキュリティと容易な利用をサポートする領域において、実施すべき作業を明示するものとなる。

Similarly, this document proposes an ideal Enterprise hub architecture which is not yet in the marketplace. This is with the intention of stimulating and informing future product design, development and implementation.

同様に、このドキュメントでは、現時点でマーケットに登場していない、理想的なエンタープライズ・ハブ・アーキテクチャが提案される。つまり、将来における製品の設計／開発／実装を、促進することを目的としている。

Further work can be done to apply hub thinking to existing implementation approaches and identification and adoption of key industry standards to support a hub architecture. Before standards solutions are available, Enterprises should be able to identify the primary IoT and security management needs for their organization by using this Hub architecture in conjunction with a comprehensive risk assessment. With this information, Enterprises may then identify those available market solutions that are best suited for their own IoT deployment.

ハブの発想を既存の実装アプローチに適用し、ハブアーキテクチャをサポートする主要な業界標準を識別／採用することで、作業の領域を拡大することができる。こうした標準的ソリューションが利用可能になる前に、企業が特定すべきことは、包括的なリスク評価と組み合わせたハブ・アーキテクチャを使用することで生じる、主要IoTおよびセキュリティ管理のニーズとなる。ここで提供される情報を活用することで、それぞれの企業におけるIoTデプロイメントに最適な、市場のソリューションを特定できるようになる。

1.2 Scope

The focus of this document is the definition of a Hub-based architecture for IoT devices and solutions implemented and managed by the Enterprise.

このドキュメントがフォーカスするのは、エンタープライズで実装／管理されるIoTデバイス／ソリューションのための、Hub_Baseアーキテクチャの定義である。

We do not make assumptions about the business models of enterprises or IoT solution providers. For this particular reference architecture, it is assumed that IoT devices will not be wholly owned, controlled and operated by the IoT provider – as is the case in some business models. Instead it is assumed the relevant devices will have some level of ownership, control and management by the enterprise itself.

ただし、ここでは、企業やIoTソリューション・プロバイダーのビジネス・モデルについては想定していない。この、限定されたリファレンス・アーキテクチャでは、いくつかのビジネス・モデルに散見されるように、IoTプロバイダーにより個々のIoTデバイスが、完全に所有／制御／運用されることはないと想定している。それに代えて、関連するデバイスは企業自体により、所有／制御／管理されると想定している。

Below is a more detailed list of IoT and related issues considered in scope of this proposed Hub architecture:

ここで提案されるハブ・アーキテクチャの範囲で考慮されるIoTおよび、関連する問題の詳細なリストを以下に示す。

- Consumer, in addition to Enterprise-focused, IoT solutions
- Devices that connect to and/or provide information via the Enterprise's network
- Devices with security features that are managed by the Enterprise (e.g. authentication, roots of trust, password control, update)
- Devices with configuration options managed by the Enterprise

- エンタープライズ向けのIoTソリューションと、消費者向けのIoTソリューション
- 企業のネットワークに接続し、情報を提供するデバイス
- エンタープライズにより管理される、セキュリティ機能を備えたデバイス（認証、信頼のルーツ、パスワード制御、更新など）
- 企業が管理する、コンフィグレーション・オプションを備えたデバイス

The scope of the Enterprise IoT category could be very broad. Explicitly we do not include details regarding specific deployments of IoT, such as Enterprise building fabric solutions like Building Information Modelling (BIM). A deployment such as BIM could warrant its own architecture and special considerations. Instead, the architecture focuses on more general and common uses of IoT solutions such as smart office applications (defined broadly, ranging from connected printers to smart whiteboards), operational efficiency (such as IoT telemetry) and/or smart manufacturing systems. This is to focus effort on covering the majority of enterprise use cases and to concentrate on the IoT devices available for sale today or those widely anticipated, as most enterprises will be looking at the current and future markets for their technology solutions.

エンタープライズIoTカテゴリの範囲は、大きく広がる可能性を持つ。したがって、このドキュメントでは、エンタープライズ・ビルディング・ファブリック・ソリューションである Building Information Modelling (BIM) などの、特定IoTの詳細な展開については除外している。BIMなどの展開では、独自のアーキテクチャに加えて、特別な考察が必要になる場合があるり。その一方で、ここで説明するアーキテクチャは、たとえばスマート・オフィス・アプリケーション（接続されたプリンターからスマート・ホワイト・ボードに至るまで）や、運用効率（IoTテレメトリなど）、スマート製造システムなどの、より広義で一般的なIoTソリューションの活用に焦点を当てている。それは、企業における大部分のユースケースをカバーすることに注力し、現時点で販売され期待を集めているIoTデバイスに集中することになる。なぜなら、ほとんどの企業が、自身のテクノロジー・ソリューションを現在と未来の市場に適用したいと考えるからである。

Below is a more detailed list of IoT and related issues considered out of scope for this proposed Hub architecture:

以下のリストは、ここで提案されるハブ・アーキテクチャの範囲外と見なされる。IoTに関連する領域や要素の詳細である。

- The specific requirements for the following sectors are not in scope
  - Building management
  - Building information modelling
  - The adaptation or augmenting of legacy IoT device capacities
  - BYOD devices broadly (such as personally owned smart fitness devices)
  - Fleet vehicles and mobile assets

- 以下の分野における特定の要件は範囲外とする
  - ビルディング・マネージメント
  - ビルディング情報モデリング
  - 能力が不足しているレガシーIoTデバイスの適用と補完
  - BYOD デバイス (個人が所有するフィットネス・デバイスなど)
  - Fleet vehicles and mobile assets

- Other Considerations not in scope
  - Existing BYOD devices that IT departments already provide for, such as visitor's laptops
  - Consideration for sector-specific requirements and regulations – such as security and data protection requirements for the finance, healthcare, or critical national infrastructure sectors
  - Sub architectures for this and other IoT reference models: the specific IoT sub architecture within the Hub ecosystem is unique to each deployment. This Hub-based architecture does not specify or make assumptions about sub architecture characteristics such as how and when devices are connected, traffic routing, or implementation of multiple Hub solutions
  - Procurement language and model contracts for the procurement of such hub equipment

- 以下の考察は範囲外とする
  - 訪問者のラップトップなど、IT部門がすでに提供している既存のBYODデバイス
  - 金融／医療／行政インフラストラクチャなどにおける、セキュリティやデータ保護性などの、固有の要件および規制に関する考慮事項
  - ここで説明するIoTリファレンス・モデルおよび、他のIoTリファレンス・モデルのサブアーキテクチャ。ハブ・エコシステム内の特定IoTサブ・アーキテクチャは、それぞれが個別／固有にディプロイされる。このHub_baseアーキテクチャでは、たとえばデバイスの接続方法とタイミングや、トラフィック・ルーティング、複数のハブソリューション実装などの、サブ・アーキテクチャの構造を特定／想定していない。
  - ハブ機器などを調達するのための調達言語とモデル契約

1.3 Intended Audience

The intended audience for this document is for people with the following roles or responsibilities:

このドキュメントの対象読者は、次の役割または責任を持つ人々である。

- CxOs and IoT purchasers – to better inform purchasing decisions, particularly:
  - Section 1: Purpose
  - Section 2: Overview
- IT departments – to better inform security-focused Enterprise IoT management and architecture, particularly
  - Section 2: Overview
  - Section 3: Hub-Based Reference Architecture
- Developers – to better understand IoT management and security needs of Enterprises and gaps in the market, particularly:
  - Section 3: Hub-Based Reference Architecture
- OEM Product Management – to better understand IoT management and security needs of Enterprises and gaps in the market, particularly:
  - Section 3: Hub-Based Reference Architecture

- CxOs and IoT purchasers – 購入に関する、より良い意思決定のために
  - Section 1: Purpose
  - Section 2: Overview
- IT departments – Enterprise IoT を管理／構築する際の、適切なセキュリティの実化のために
  - Section 2: Overview
  - Section 3: Hub-Based Reference Architecture
- Developers – Enterprises におけるIoT管理とセキュリティの必要性、そして市場のギャップを理解するために
  - Section 3: Hub-Based Reference Architecture
- OEM Product Management – Enterprises におけるIoT管理とセキュリティの必要性、そして市場のギャップを理解するために
  - Section 3: Hub-Based Reference Architecture

1.4 Taxonomy

In the requirements sections, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119 [ref 2].

The following terms are used in this document:

- Public Roots of Trust: A publicly trusted root is one whether the root of trust is publically accessible, typically where the trust anchor is publically published by one of the public Certificate Authorities
- Private Roots of Trust: A private root differs from a public root because roots of trust aren't publically accessible. The root(s) of trust will need to be published by the organization whose Certificate Authority created the root of trust, to those entities which need to validate the chain of trust anchored by the private root

2 Overview

There are two key elements to the proposed architecture: the Hub device and the flexible Hub networking model. The Hub device acts as a central point for trust and network management. It also adds an additional layer of security to the IoT environment. The Hub device supports flexible networking by allowing IoT devices and sub-architectures to be deployed in the IoT environment as preferred by the Enterprise. Thus, it does not propose particular network architectures beyond separating IoT[1] and business networks.[2]

ここで提案されるアーキテクチャには、2つの重要な要素として、ハブ・デバイスと柔軟なハブ・ネットワーク・モデルがある。ハブ・デバイスは、信頼とネットワーク管理の中心として機能する。 また、IoT環境にセキュリティ層を追加する。このハブ・デバイスが、柔軟なネットワークをサポートすることで、企業のニーズに応じたIoTデバイスとサブ・アーキテクチャを、IoT環境にディプロイできるようになる。したがって、IoTネットワークとビジネス・ネットワークを分離する以外に、特定のネットワーク・アーキテクチャを提案することはない。

Unlike other IoT architectures, this Hub architecture provides a centralized point for IoT device and network management utilizing existing security features and offering flexible solutions for the Enterprise. The Hub supports IoT managers by aggregating information and communicating with relevant network elements such as routers and IoT devices. It may also adopt additional functions, for instance acting as a gateway. This enables information sharing between the local IoT environment and other networks or entities, such as the IoT smart coffee machine provider.

他のIoTアーキテクチャとは異なり、このハブ・アーキテクチャでは、対象となるエンタープライズにおける既存のセキュリティ機能と柔軟なソリューションを活用するために、IoTのデバイスとネットワークを管理のための、センタライズされたポイントを提供する。このハブは、ルーターやIoTデバイスなどの関連するネットワーク要素と通信し、情報を集約することで、IoTマネージャーをサポートする。また、たとえばゲートウェイ機能などの、特定の機能を追加する場合もある。それにより、ローカルIoT環境と、他のネットワークやエンティティとの間で情報共有が可能となる。極端な話、IoTスマート・コーヒーマシン・プロバイダーなどとの通信も可能になる。

For added security, it is recommended that Enterprise IoT devices connect via a dedicated IoT network and not via the business network. The aim is to minimize the Enterprise and IoT network attack surfaces by protecting business operations from IoT devices which may be used as an attack vector.

セキュリティを強化するために、企業内のIoTデバイスの接続は、ビジネス・ネットワークではなく、専用のIoTネットワークを介して行われる形態が推奨される。その目的は、攻撃ベクターとして悪用される可能性のあるIoTデバイスからビジネス・オペレーションを保護し、エンタープライズおよびIoTネットワークの攻撃対象領域を、最小限に抑える点にある。

It is believed that, compared to other architectures, this Hub architecture offers a more secure and easy to manage Enterprise IoT ecosystem. The Hub architecture is also intended to be a flexible solution to fit any size or type of Enterprise deployment. Flexibility allows the Enterprise to adopt the best IoT solution to suit its needs while not compromising on security. For example, the ability to choose which data is kept within the organization (e.g. managing sensitive data on the Hub) and when to use cloud solutions.

このハブ・アーキテクチャは、他のアーキテクチャと比較して、より安全で管理しやすいエンタープライズIoTエコシステムを提供すると考えられる。ハブ・アーキテクチャは、あらゆるサイズまたはタイプのエンタープライズ・デプロイメントに適合する、柔軟なソリューションになることも目的としている。この柔軟性により、企業はセキュリティを犠牲にすることなく、ニーズに合わせた最適なIoTソリューションを適用できる。たとえば、組織内に保持するデータ（ハブによる機密データの管理など）や、クラウド・ソリューションなどを、どのように活用するのかを選択する能力が得られる。

For more information on the benefits of a Hub architecture, see section *2.2.2 Why a Hub?* and *Table 1: Architecture Characteristics*

ハブ・アーキテクチャの詳細なメリットについては、section 2.2.2 Why a Hub? と Table 1: Architecture Characteristics を参照のこと。

2.1 Hub-based Reference Architecture

Enterprises and their IoT deployments differ and the proposed Hub architecture is intended to provide a flexible solution which can accommodate a wide variety of Enterprise environments. It is not intended to address a single device/interface solution. Instead it enables the implementation of a collection of security and trust tools that support IoT deployment and management in different Enterprise environments and IoT solutions. For instance, small enterprises may only require a single Hub while larger enterprises will most likely need a number of Hubs – both for scalability and redundancy. Because of its central role, the Hub provides a point to oversee, monitor, and, to a degree, control the Enterprise's local IoT ecosystem.

企業自身と、そのIoTデプロイメントは切り分けて考える必要があり、また、ここで提案されるハブ・アーキテクチャは、さまざまな企業の環境に対応が可能な、柔軟なソリューションの提供を目的としている。単一のデバイス／インターフェイスによるソリューションへの、対応を目的とはしていない。それに代えて、さまざまなエンタープライズ環境およびIoTソリューションにおいて、IoTの展開と管理をサポートするセキュリティとトラスト・ツールの、コレクションの実装を可能にする。たとえば、中小企業はシングル・ハブのみを必要とするだろうが、大企業はスケーラビリティと冗長性を担保するために、マルチ・ハブを必要とする場合がある。その中心的な役割を担うハブは、エンタープライズにおけるローカルIoTエコシステムを監視し、ある程度の制御も実現するためのポイントを提供する。

The Hub is central to the reference architecture, aggregating information and communicating directly with other devices and network elements in the IoT environment. At the same time, the Hub can be visualized at the edge of a network, providing a secure gateway for communication between networks. The Hub should be user-friendly and support good device management and security practices. It should integrate seamlessly with existing network management tools and cater to IoT managers with a variety of capabilities and backgrounds. In addition, the Hub itself needs to have robust security to protect the information and roots of trust that it manages.

ハブはリファレンス・アーキテクチャの中心であり、IoT環境内のデバイスやネットワーク要素などとダイレクトに通信し情報を集約する。それ同時に、ハブはネットワークのエッジで視覚化され、ネットワーク間の安全な通信のためのゲートウェイを提供する。ハブはユーザー・フレンドリーであり、また、優れたデバイス管理とセキュリティ・プラクティスをサポートする必要がある。さらに、既存のネットワーク管理ツールとのシームレスな統合を実現し、IoTマネージャーが持つ多様な能力と背景に対応する必要がある。加えて、ハブは、自身が管理する情報と、信頼のルーツを保護するために、堅牢なセキュリティを備える必要がある。

[1] For the purpose of this architecture, an IoT network is a network dedicated to supporting IoT solutions deployed in the enterprise environment. For instance, this may include smart light bulbs, motion detectors, manufacturing equipment, or smart coffee machines.

[2] For the purpose of this architecture, a business network is a network (local or wide area) which enables normal business functioning of the enterprise, such as employee access to servers and document stores, enables internet and email access, and direct communications with vendors or clients.

This Hub architecture provides another layer of security for both the wider network and for those devices that may have minimal or no built-in security features by considering security at every level. As a result, the Hub architecture is proposed as a more robust and secure architecture than others, such as “tree” or “hub-and-spoke”.

このハブ・アーキテクチャは、多様なネットワークとデバイスの双方に対して、セキュリティのためのレイヤを提供する。そして、すべてのレベルにおけるセキュリティを考慮することで、セキュリティ機能が組み込まれていないデバイスなどにも対応していく。その結果として、ハブ・アーキテクチャは、ツリーやハブ・アンド・スポークなどのアーキテクチャと比較して、より堅牢で安全な環境を提案する。

As opposed to a tree network, which connects a number of nodes via a direct communication line without a central management point, the Hub provides an information aggregation point for all devices or groups of devices and other Hubs such as gateways deployed within the local IoT network. Additionally, the Hub device itself, not only the network architecture, is a key information aggregation element required to fully implement the proposed architecture.

センタライズされた管理ポイントを持たずに、ダイレクトに多数のノードを接続するツリーネット・ワークとは対照的に、ハブは情報集約ポイントを提供する。そこには、すべてのデバイスと、デバイスのグループ、そして、およびローカルIoTネットワーク内にディプロイされたゲートウェイなどのハブが接続される。さらに、ハブ・デバイス自体は、ネットワーク・アーキテクチャとして機能するだけではなく、アーキテクチャを完全に実装するために必須の情報を集約する要素となる。

Unlike a hub-and-spoke model, the devices in the Hub architecture do not rely on the Hub to talk to other devices or execute its functions. But the Hub does provide a management point where requests or actions can be taken, communicating from one to many and vice versa.

ハブ・アンド・スポーク・モデルとは異なり、ハブ・アーキテクチャのデバイスは、他のデバイスとの通信および、自身の機能の実行を、ハブには依存しない。ただし、このハブは、リクエストやアクションの実行が可能な管理ポイントを提供し、one to many の相互通信を行う。

2.2 Aim of Hub Architecture

This Hub reference architecture aims at providing a user-friendly centralized management solution for Enterprises deploying IoT devices and solutions – from one or multiple vendors. Importantly, the architecture considers security a primary objective and provides a way forward with this in mind. The desired result is a more secure IoT ecosystem within Enterprise environments that is user-friendly, easy to deploy and manage. Enterprises should be able to adopt this Hub architecture as well as use it as part of proof of compliance. It is also intended to highlight where security solutions currently available on the market fulfil as well as lack these desired features.

このハブ・リファレンス・アーキテクチャは、単一／複数のベンダーから構成されるIoTのデバイス／ソリューションをディプロイする、企業のためのユーザー・フレンドリーな集中管理ソリューションの提供を目的とする。重要なことは、このアーキテクチャではセキュリティが主要な目的と見なされ、それを念頭に置いた実装方式が提供される点にある。結果として望まれるのは、エンタープライズ環境内のより安全なIoTエコ・システムであり、また、ユーザーフ・レンドリーであり、ディプロイと管理を容易にすることである。対象企業は、このハブ・アーキテクチャを採用できるだけではなく、proof of compliance の一部として用いることも可能である。また、現時点のマーケットで入手可能なセキュリティ・ソリューションで満たされる領域と、そこで不足している機能への要求を、明らかにすることも目的とする。

2.2.1 Main Hub Functions

In this Hub-based reference architecture, the Hub is a centralized IoT management point with the ultimate aim of supporting trust and security within the Enterprise's IoT deployment. The Hub provides a central point to oversee and monitor – but not necessarily directly control – every aspect of the IoT ecosystem. This is done by providing a device and user interface that can act as a repository of information for monitoring, audit and reporting capabilities, provide alerts and notifications, act as a certificate manager and/or cache, provide access controls, and possibly device control functionalities. In essence, the Hub functions as an IT manager resource.

このHub-based リファレンス・アーキテクチャでは、対象となるハブはセンタライズされたIoT管理ポイントとなり、エンタープライズIoTデプロイメントにおける、トラストとセキュリティのサポートを究極の目的とする。このハブは、IoTエコシステムのあらゆる側面を監督／監視するための中心点を提供するが、必ずしもダイレクトに制御する必要はない。具体的に言うと、監視／監査／報告のための情報リポジトリとして機能し、また、アラートと通知を提供できる、デバイスとユーザー・インターフェイスの提供により実現される。さらに、証明書マネージャーやキャッシュとして機能し、アクセス制御およびデバイス制御の機能を提供することもある。本質的に、このハブは、ITマネージャーのリソースとして機能する。

To enable the Hub's flexible management of a unique Enterprise IoT ecosystem, it supports three basic IoT device "classes". Of the three classes listed below, most IoT devices will fall in Class 2, where the Enterprise may centralize as much of the device management as possible within the Hub architecture, but some aspects of management may rest with the service provider.

それぞれのエンタープライズIoTエコシステムにおいて、ハブによる柔軟な管理を可能にするために、基本的には3つのIoTデバイス Class がサポートされる。大半のIoTデバイスは、以下のリストの Class 2に分類される。ハブ・アーキテクチャ内の大半のデバイス管理は、エンタープライズによりセンタライズされるが、管理の一部はサービス・プロバイダーに依存する場合がある。

- **Class 1: Fully controlled and connected** – where interfaces such as IoT device control, data collection and management are fully integrated and controlled by the Hub device and kept within the Enterprise
- **Class 2: Partially controlled and/or connected** – where the Hub device may execute some but not all interfaces with the device, such as pushing updates and managing traffic but not collecting sensor data
- **Class 3: Information sharing** – the most basic type of interaction, the Hub would not control or manage the IoT device functions such as updating or data collection, but instead will log basic information such as device status or installed updates

- **Class 1: Fully controlled and connected** – IoTデバイスの制御および、データの収集／管理などのインターフェースは、ハブ・デバイスにより完全に統合／制御され、エンタープライズ内に保持される。
- **Class 2: Partially controlled and/or connected** – ハブ・デバイスは、対象となるデバイスのインターフェイスを介して、アップデートのプッシュやトラフィックの管理などを実行するだろうが、センサー・データの収集などは行わない。
- **Class 3: Information sharing** – 最も低位のインタラクションが行われる。IoTデバイス機能のアップデートのやデータ収集などのを制御／管理は行われないが、デバイス・ステータスやインストール済みのアップデートのなどの、基本的な情報をログに記録する。

For the purpose of this architecture, the main Hub functions or support capabilities include network management, connecting devices securely, and lifecycle management. Below are examples of how each of these Hub functions support Enterprise IoT security:

ハブの主要な機能およびサポートする機能には、このアーキテクチャの目的である、ネットワーク管理／デバイスの安全な接続／ライフサイクル管理が含まれる。以下の例は、こうしたハブの機能が、個々のエンタープライズIoTセキュリティをサポートする方式を示している。

- **Network Management and Security Tools**
  - **Local IoT Network**: Implementing a local IoT Network to separate traffic, minimize attack surface and protect business operations [see section 3.2.1]
  - **Separation of Testing, Staging and Live Systems**: Separating systems to reduce the risk of new devices reducing the security of the IoT ecosystem [see section 3.2.2]
  - **Gateways and Firewalls:** Implementing gateways and firewalls to protect networks and data, and manage traffic [see section 3.2.3]
- **Connecting Devices Securely**
  - **Authentication and Authorization**: Using authentication and authorization to ensure only verified and permitted devices are on the network [see section 3.3.1]
  - **Secure Boot**: Using secure boot to validate the integrity of IoT software [see section 3.3.2]
  - **Roots of Trust**: Implementing roots of trust to support security foundation [see section 3.3.3]
- **Lifecycle Management**
  - **Monitoring and Audit**: Using monitoring, discovery and audit tools to oversee the IoT ecosystem, [see compliance prove and decisions, informed on based action takes section 3.4.1]
  - **Update and Patch**: Managing update and patch processes and history to support security best practice throughout the device lifecycle [see section 3.4.2]
  - **Manage Device Identity and Authorization:** Using device identity to manage and improve security of devices, including end-of-life provisioning [see section 3.4.3]
  - **Managing End-Of-Life**: Managing device end-of-life securely for scenarios including device end-of-support, replacement, and ownership transfer [see section 3.4.4]

- **Network Management and Security Tools**
  - **Local IoT Network:** ローカルIoTネットワークを実装してトラフィックを分離し、攻撃対象領域を最小限に抑え、ビジネス・オペレーションを保護する [see section 3.2.1]
  - **Separation of Testing, Staging and Live Systems:** システム間を分離して、新規デバイスの追加によるIoTエコ・システムのセキュリティを低下リスクを軽減する[see section 3.2.2]
  - **Gateways and Firewalls:** ゲートウェイとファイアウォールの実装により、ネットワークとデータを保護し、トラフィックを管理する[see section 3.2.3]
- **Connecting Devices Securely**
  - **Authentication and Authorization**: 認証と承認を用いて、検証／許可されたデバイスのみがネットワーク上にあることを確認する [see section 3.3.1]
  - **Secure Boot**: セキュア・ブートを用いて、IoTソフトウェアの完全性を検証する[see section 3.3.2]
  - **Roots of Trust**: 信頼のルーツを実装し、セキュリティ基盤をサポートする[see section 3.3.3]
- **Lifecycle Management**
  - **Monitoring and Audit:** 監視／発見／監査ツールを用いてIoTエコシステムを監督し、情報に基づいた行動を起こし、コンプライアンスを証明する [see section 3.4.1]
  - **Update and Patch**: パッチの処理／履歴を管理することで、デバイ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・プラクティスをサポートする [see section 3.4.2]
  - **Manage Device Identity and Authorization:** デバイスIDを用いて、サポート終了のプロビジョニングも含めて、デバイスのセキュリティを管理／改善する[see section 3.4.3]
  - **Managing End-Of-Life**: デバイスのサポート終了シナリオを管理し、個々のデバイスに関する交換や所有権の譲渡を含めて、デバイスの寿命を安全に管理する[see section 3.4.4]

2.2.2 Why a Hub?

This paper proposes a Hub-based architecture as a robust foundation for IoT security and management for several reasons, including:

このホワイト・ペーパーでは、IoTのセキュリティを管理する堅牢な基盤としての、Hub-basedアーキテクチャを提案する。理由としては、以下の項目などが含まれる。

- **Centralized Management** – A Hub is characterized as the focal point in a network, with connectivity to all groups/devices, network management tools or other Hubs. Ideally, this Hub would enable IoT ecosystem lifecycle management by supporting network and end-device security. It provides an easy one-stop-shop to manage roots of trust, monitor network traffic, devices on the network, and updates and patches
- **Software Update and Patch** – The failure or inability to update connected devices is a now well-known security risk [see ref 11]. A Hub would enable the management and implementation of software updates within the Enterprise IoT ecosystem and offer high-level update-able management Hub to protect those devices without update capabilities. It would also facilitate an additional layer of security by providing an easy update point particularly for those devices which do not support endpoint solutions such as updating and patching
- **Security Compliance** – A Hub architecture provides a central place to manage layered security and ensure a minimum level of security that protects all IoT devices across the Enterprise. In addition, it could assist with regulatory compliance. For instance, the Hub could act as a firewall and/or provide a simple update and patch mechanism. The Hub can enable, log, and report on security features or statuses, providing a repository of information that may be used to prove compliance with standards or regulations as needed
- **Troubleshooting** – A Hub would also provide an easy troubleshoot mechanism for the Enterprise IoT ecosystem. The ability to manage, audit and monitor traffic and connected devices in one central place supports IoT security management. This not only helps manage devices, but also provide real- time notifications of malicious devices, network anomalies and pinch-points

- **Centralized Management** – ネットワークの中心点として特徴付けられたハブは、すべてのグループ/デバイスおよびネットワーク管理ツールなどに接続する。このハブは、ネットワークとエンドデバイスのセキュリティをサポートすることで、IoTエコシステムのライフサイクル管理を可能するのが理想である。それにより、信頼のルーツを管理し、ネットワーク・トラフィックおよび、ネットワーク上のデバイス、そしてアップデート／パッチを監視するための、簡単なワン・ストップ・ショップが提供される。
- **Software Update and Patch** – 接続されたデバイスの更新が失敗／不能であることが、セキュリティ・リスクになることは、いまでは広く認識されている [ref 11を参照]。ハブにより、エンタープライズIoTエコシステム内での、ソフトウェア・アップデートの管理／実装が可能になる。また、それらのデバイスのアップデート機能に依存することなく、ハイ・レベルのアップデート管理が実現される。アップデート／パッチの適用といったエンドポイント・ソリューションをサポートしないデバイスに対して、簡潔なアップデート・ポイントを提供することで、セキュリティのためのレイヤー追加を促進する。
- **Security Compliance** – ハブアーキテクチャは、階層化されたセキュリティを管理するための中心点を提供し、エンタープライズにおける全IoTデバイスを保護するための、最小レベルのセキュリティを確保する。さらに、コンプライアンス順守に役立つ可能性もある。 たとえば、ハブはファイアウォールとして機能し、単純なアップデート／パッチ・メカニズムを提供することもある。このハブにより、セキュリティの機能とステータス関するログへの記録／報告が有効となり、スタンダードおよびコンプライアンスへの準拠を、必要に応じて証明するための情報リポジトリを提供される。
- **Troubleshooting** – このハブは、エンタープライズIoTエコシステムにおける、簡潔なトラブル・シューティングメカニズムも提供する。トラフィックと接続されたデバイスを、一元的に管理／監査／監視する機能が提供され、IoTセキュリティの管理がサポートされる。つまり、デバイス管理に役立つだけでなく、悪意のあるデバイスやネットワークの異常／弱点を、リアルタイムに通知する機能も提供される。

In addition to the security and management attributes, a Hub-based architecture is also considered highly flexible to accommodate a variety of Enterprise implementations. A quick comparison of network architecture characteristics (below) highlights the security functions and flexibility that the Hub architecture offers.

セキュリティ機能と属性の管理に加えて、このHub-Basedアーキテクチャは、各種のエンタープライズにおける実装に対応するための、高度な柔軟性を提供すると思われる。以下に示す、ネットワーク・アーキテクチャごとの特性比較を見れば、ハブ・アーキテクチャが提供するセキュリティ機能と柔軟性が浮き彫りになる。

Architecture Characteristics	Hub Architecture	Tree Network	Hub-and-Spoke or Star Networks	Mesh Network	Ring Network
Supports a centralized network management tool	X	X	X		
Supports hybrid network sub-architectures	X	X	X		
Supports direct communication with management tool (does not require information to travel through unneeded nodes or pathways)	X	X	Sometimes		
Information must be shared in a hierarchical manner		X	X		
Network management tool is resilient to device and network disruptions	X	X		X	
In the event of management point failure, networks and devices can continue functioning	X			X	
Central management and information aggregation point	X				
Management tool supports IoT device identity, access and authorization resources	X				
Management tool supports minimization of attack surface	X		X		
Dedicated device for network and IoT device management	X				

Table 1: Architecture Characteristics

2.3 Assumptions

2.3.1 Device Ownership

We assume devices will have a mix of privilege and variety of ownership, by visitors and employees of the enterprise and the enterprise itself. Devices may be used by many people and require trust properties to reflect this, but without imparting administrative privileges to all users of that device.

一連のデバイスには、多様な特権と所有権が混在し、企業における訪問者と従業員や、その企業などに分類されると想定している。それらのデバイスは、数多くの人により使用される可能性があるため、トラスト・プロパティが必要になるが、すべてのデバイスのすべてのユーザーに対して、管理者権限を付与する必要はない。

2.3.2 Network Security

We assume a relatively static size of network, but one that might be expanded to incorporate new technologies as they are rolled out. The need to manage such a diversity of devices is recognized, with an emphasis on clarity of device statuses across the network, and simplicity in the process for improving and updating network security.

ネットワークの規模は、それほど動的なものとは想定されていないが、新しいテクノロジーが展開されるにつれて、それらを組み込むために拡張される可能性がある。また、多様なデバイスの管理などが必要だと認識されているが、ネットワーク全体のデバイス・ステータスの明確さや、ネットワークセキュリティの改善と更新のプロセスの簡素化などにも、重点を置く必要がある。

2.3.3 Visitor Access

In addition, each enterprise should have strong and established trust policies for devices and groups of devices, such as visitor or guest devices, including levels of trust. This includes temporary Enterprise devices which may be connected to the business as opposed to the guest network. In cases such as these, it assumed that the Enterprise will manage access and device privileges in alignment with Enterprise policy. Whilst specific recommendations on such policies are outside the scope of this document – they will be individual to the needs and security requirements of each enterprise – we do assume that an enterprise will offer open connectivity to visitor devices, so that they will have access to connectivity, but no administrative privileges.

さらに、それぞれの企業は、デバイスおよびデバイス・グループ（訪問者またはゲストデバイスなど）に対する信頼のレベルを含め、強力で確立されたトラスト・ポリシーを持つ必要がる。そこには、ゲスト・ネットワークではなくビジネス・ネットワークに接続できる、テンポラリーなエンタープライズ・デバイスも含まれる。このような場合、エンタープライズ・ポリシーに従って、アクセスとデバイスの特権が管理されることが前提になる。このようなポリシーに関する特定の推奨事項は、当ドキュメントの範囲外となり、それぞれの企業のニーズとセキュリティの要件に応じた個別のものとなる。ここでの想定は、それぞれの企業において、ビジター・デバイスに対するオープンな接続を提供されるが、管理者権限は提供されないというものである。

2.3.4 Privileges

We assume that a variety of device/service access and administrative privileges will be managed by the enterprise. Administrative privileges will be influenced by a variety of factors such as the device class (as specified in section 2.2.1), IoT solution business model, handling of business critical and sensitive data, and technical capacity within the organization. We also assume that general users will not be restricted from using the device's full functionality, yet at the same time they do not have administrative privileges. For example, a person should be able to make full use of a smart coffee machine and its services – for example save their regular coffee order and gift coffees to others – whilst not being able to access free test coffee drinks.

ここでの前提は、各種のデバイス／サービスへのアクセスおよび管理者権限が、エンタープライズにより管理される形態である。管理特権は、さまざまな要因の影響を受ける。具体的に言うと、デバイス・クラス（セクション2.2.1を参照）や、IoTソリューションのビジネス・モデル、ビジネスに不可欠で機密性の高いデータの処理、組織内の技術的能力などが挙げられる。また、一般ユーザーはデバイスの全機能の使用を制限されないが、それと同時に管理者権限を持たないことも前提となる。たとえば、ある人はスマート・コーヒーマシン・サービスを最大限に活用できる必要がある。つまり、レギュラー・コーヒーの注文やギフト・コーヒーの発行を可能にするが、無料のテスト・コーヒー・ドリンクにアクセスすることはできない。

2.3.5 Sector-Specific Requirements

Enterprises in certain industry sectors will have more regulation constraints than others, and so there will be a variance in security and audit requirements between enterprises. We assume that the enterprise will adhere to sector-specific requirements including regulations and best practices.

特定の業界に所属する企業には、他の業種と比較してより多くの規制があるため、企業ごとのセキュリティと監査の要件は一様ではない。ここでの前提は、それぞれの企業が、規制やベスト・プラクティスなど含む、業界固有の要件を順守することである。

2.3.6 Technologically Neutral

This proposed Hub architecture is intended to be technology agnostic, and therefore should be flexible and broadly applicable to IoT deployments. It is important to keep in mind that the business models of IoT solutions, particular enterprise structures, and unique deployments will all impact implementation of this architecture. Therefore, the following is provided as an example and not a rigid implementation of the architecture described here. Where existing protocols or standards are referenced for illustration and are in not intended to be prescriptive references.

ここで提案されるハブ・アーキテクチャは、テクノロジーに捉われない柔軟性を持ち、IoTデプロイメントに広く適用できなければならない。IoTソリューションのビジネス・モデルや、エンタープライズ固有の構造、それぞれのデプロイメントが、このアーキテクチャの実装に影響を与えることを覚えておく必要がある。したがって、以下の説明は例として提供されるものであり、また、ここで説明するアーキテクチャの厳密な実装ではない。既存のプロトコルやスタンダードは、説明のために参照されており、規範としての参照を意図するものではない。

2.4 Security Principles

There is a huge variety of devices labelled “IoT” and equal variety in the level of security features supported by those devices and solutions. Enterprises need to be aware of security risks when implementing IoT solutions, and therefore should be aware of common security principles, no matter the deployment environment. The resulting decisions will most likely differ by Enterprise as no IoT deployment is the same. Nevertheless, these principles should be taken into consideration from the outset.

IoTとラベル付けされた多様なデバイスがあり、それらのデバイスとソリューションでサポートされるセキュリティ機能のレベルも多様である。企業は、IoTソリューションを実装する際にセキュリティリスクを認識する必要があるため、デプロイメント環境に関係なく、一般的なセキュリティ原則を認識する必要がある。同一のIoTデプロイメントは存在しないため、結果として得られる決定事項は、それぞれの企業による異なるものになるだろう。それであっても、以下の原則は、最初から考慮に入れる必要がある。

The most modest approach to security focuses on the following three key principles, also included in the “IoT Security Comliance Framework” [ref 1]

セキュリティへの最も控えめなアプローチは、IoT Security Comliance Framework [ref 1] にも含まれている、以下の3つの主要原則に焦点を当てるものとなる。

- Confidentiality – ensuring information and systems are protected from unauthorized access
- Integrity – ensuring that information and systems are unaltered and accurate throughout the lifecycle. For instance, information integrity applies to data collection, transfer, use and storage
- Availability – ensuring that information is and services are accessible by users or systems as and when needed

- Confidentiality – 情報とシステムが、不正アクセスから保護されていることの確認
- Integrity – 情報とシステムが、ライフサイクル全体を通じて変更されず、正確であることの確認。たとえば、情報の完全性は、データの収集／転送／使用／保存に適用される
- Availability – 必要に応じて、ユーザーとシステムが情報とサービスにアクセスできることの確認。

From these principles, a wide variety of questions emerge when considering IoT solutions. Many of these questions are considered in “Make it safe to connect: Establishing principles for Internet of Things Security” [ref 10] by the IoT Security Foundation, replicated here for ease:

これらの原則から、IoTソリューションを検討する際の、さまざまな疑問が浮かび上がる。これらの質問の多くは、IoT Security Foundation による Make it safe to connect: Establishing principles for Internet of Things Security [ref 10]で検討されているが、以下で簡単に紹介する。

- Does the data need to be private?
- Does the data need to be audited?
- Does the data need to be trusted?
- Is the safe / timely arrival of data important?
- Is it necessary to restrict access to, or control of, the device?
- Will the device need to be updated?
- Will ownership of the device need to be managed or transferred?

- データはプライベートである必要があるか？
- データを監査する必要があるか？
- データに対する信頼は必要か？
- データのセキュアでタイムリーな到着は重要か？
- デバイスへのアクセスと制御を制限する必要があるか？
- デバイスのアップでに関する必要性はあるか？
- デバイスの所有権に関する管理／譲渡が必要になるか？

Developing these points to take into consideration architectures as well as data security, this proposed Hub architecture expands upon the list above. The following architecture-specific questions are incorporated here:

アーキテクチャだけではなくデータ・セキュリティを考慮に入れるために、以下のポイントを発展させることで、ここで提案されるハブ・アーキテクチャは上記のリストを拡張する。次のアーキテクチャ固有の疑問が、ここには組み込まれている。

- What is the Hub's relationship with trust management? [see section 3.3.3]
- How does the Hub architecture support layered security? [see section 3.2]
- To what extent is network access managed and when should access be revoked? [see section 3.2.1]
- Where is it safe to make the data transparent for monitoring, updating and auditing? [see section 3.3]
- What permissions are given to a device and does it – and potentially its data – need to be treated differently to other devices? [see section 3.3.1]
- What information about the Enterprise does the data provide, what is the relation to business-critical functions, and where is the data best managed? [see sections 3.3.1, 3.3.3]
- What should be considered when decommissioning devices or transferring device ownership? [see section 3.5]

- ハブと信頼管理との関係はどうなる？[see section 3.3.3]
- ハブ・アーキテクチャは階層化されたセキュリティをどのようにサポートする？ [see section 3.2]
- ネット・ワークアクセスはどの程度管理され、いつアクセスを取り消す必要があるか？ [see section 3.2.1]
- 監視／更新／監査のためのデータの透過性は、どこで確保すれば安全か？ [see section 3.3]
- それぞれのデバイスには、どのような権限が付与されるか？また、対象となるデバイス（場合によってはデータも含む）を、他のデバイスと異なる方法で処理する必要があるか？ [see section 3.3.1]
- データとして提供される、エンタープライズに関する情報はなにか？ビジネスク・リティカルな機能との関係および、データの最適な管理場所はどこか？ [see sections 3.3.1, 3.3.3]
- デバイスの運用が停止されるとき、また、デバイスの所有権が譲渡されるときには、何を考慮する必要があるか？ [see section 3.5]

Good security hygiene should be the foundation of any IoT management process. Therefore, the principles for this architecture are based in ensuring a minimum level of security across the Enterprise IoT ecosystem and understanding where weak points or attack vectors might be located.

セキュリティに関する適切な配慮が、IoT管理プロセスの基盤となるはずだ。したがって、このアーキテクチャ原則の基盤は、エンタープライズIoTエコシステム全体における最小レベル・セキュリティの確保と、弱点や攻撃ベクターの生じる場所の理解となる。

2.4.1 Threat Assessments and the Hub Architecture

This Hub architecture focuses on three security management features identified to support these security principles. The security management tools at the core of this architecture are:

このハブ・アーキテクチャは、上記のセキュリティ原則をサポートするために特定された、3つのセキュリティ管理機能に焦点を当てている。このアーキテクチャの中核となるセキュリティ管理ツールは、以下のとおりである。

- Network Management and Security
- Connecting Devices Securely
- Device lifecycle management

- ネットワーク管理とセキュリティ
- デバイスの安全な接続
- デバイスのライフサイクル管理

Information security is also an integral part of secure IoT ecosystems, and is supported by security management systems in the Hub architecture. It is assumed that information security best practices will be implemented with IoT deployments, be structured in a way that best meets the needs of the Enterprise, and is in compliance with relevant regulations such as local data protection and privacy regulations. Information security best practice are not the focus of the architecture, but more information on how they relate can be found in Appendix B.

情報セキュリティも、安全なIoTエコシステムにとって不可欠な部分であり、このハブ・アーキテクチャのセキュリティ管理システムによりサポートされる。ここでの前提は、情報セキュリティのベスト・プラクティスが、IoTデプロイメントと共に実装され、また、企業のニーズに最適な方法で構成され、ローカル・データ保護やプライバシー規制などの関連規制に準拠している状況である。情報セキュリティのベスト・プラクティスは、このアーキテクチャの焦点ではないが、その詳細な関連性については、Appendix B を参照してほしい。

Below is a table with a few examples to highlight the manner in which this reference architecture can help an Enterprise safeguard against some computer security threats and support compliance measures. The examples focus on the exploitation of connected systems and are organized using the widely-known STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat classification model along with two additional threats relevant to Enterprise IoT deployment – regulatory compliance and unsupported endpoint management.

以下のテーブルは、このリファレンス・アーキテクチャにより、企業が一部のコンピュータ・セキュリティ脅威から保護しされ、また、コンプライアンス評価によりサポートされるための、いくつかの例を示している。この例は、接続されたシステムの活用に焦点を当てている。広く知られているSTRIDE（Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege）脅威分類モデルに加えて、エンタープライズIoTデプロイメントに関連する、regulatory (non?) compliance と unsupported endpoint management という、2つの脅威モデルを追加している。

However, these are not the only threats to an Enterprise IoT environment, nor is it the only threat or risk model available. Other examples include: PASTA, VAST, Trike, NIST's Cyber Security Framework, NCSC's Risk Management Guidance, ISO/IEC 27000 series (particularly those on information security risk management and auditing), and OWASP (application security). An Enterprise should select the most appropriate model when executing an assessment.

ただし、エンタープライズIoT環境に影響をおよぼす脅威は。これらだけではない。そして、適用できる脅威とリスクのモデルも、これだけではない。その他の例として、PASTA, VAST, Trike, NIST's Cyber Security Framework, NCSC's Risk Management Guidance, ISO/IEC 27000 series (particularly those on information security risk management and auditing), OWASP (application security) などがある。 それぞれの企業は評価に際して、最も適切なモデルを選択する必要がある。

For a more comprehensive sample threat modelling, see Appendix A

より包括的な、脅威モデリングのサンプルについては、Appendix A を参照してほしい。

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Address resolution protocol (ARP) spoofing used to redirect data traffic to the attacker	Update and patch devices to prevent vulnerability exploitation	Authentication & Authorization [3.3.1] Update and Patch [3.4.2]
Tampering	Tampering with software to modify permissions, install spyware or backdoors	Secure boot and update to ensure software and hardware are only modified by trusted sources Periodic auditing of firmware to check for tampering or unauthorized modification	Secure Boot [3.3.2] Monitor & Audit [3.4.1]
Repudiation	Sensor data is modified in transit to the cloud service and Enterprise metrics are affected	Use of digital certificates to support secure identity of users and devices Public key infrastructure to manage and revoke digital	Authentication & Authorization [3.3.1] Roots of Trust [3.3.3]

		certificates and roots of trust	
Information Disclosure (Data Breach)	Diagnostics information shared with an OEM which discloses proprietary Enterprise information which is not required by the OEM	Traffic monitoring and management (ingoing and outgoing) Separating business and IoT networks	Local IoT Network [3.2.1] Gateway and Firewalls [3.2.3]
Denial of Service	Using exploits in connected devices to execute a DoS or DDoS attack on another IoT device in the Enterprise network	Traffic monitoring, auditing and management (on the IoT network, ingoing and outgoing) Use of gateways and firewalls to monitor and block traffic	Local IoT Network [3.2.1] Monitor and Audit [3.4.1] Update and Patch [3.4.2]
Elevation of Privilege	Unauthorized access of a cloud service provider's system enabling access to the Enterprise business or IoT network	Separation of IoT and business networks to discourage privileged users from accessing non-relevant business information	Local IoT Network [3.2.1] Authentication & Authorization [3.3.1] Monitor and Audit [3.4.1]
Regulatory non-compliance*	Need to prove compliance through metrics after a data breach to show due diligence	Log and report on security features and ecosystem management Enable security best practices Identify, manage, and update regulation compliance measures	*Highly dependent on regulatory requirements. Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Monitoring and Audit [3.4.1]
Unsupported endpoint management	Inability to encrypt data or assign a root of trust	Create a secure local environment for devices - separate devices from WAN and business networks	Local IoT Network [3.2.1] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1]

Table 2: Threat Treatment and Architecture Correlation

3 Hub-Based Reference Architecture

The architecture presented here is meant to be a resource which outlines key security considerations and how a Hub may act as a central information repository, assist IoT deployment and enable long-term management. The extent to which the Hub provides monitoring, audit and controls depends on the relevant IoT solutions, Enterprise structure, and specific implementation of this architecture.

ここで紹介するアーキテクチャは、セキュリティの重要事項を概説する、リソースとなることを目的としている。また、ハブがセンタライズされた情報リポジトリとして機能し、IoTデプロイメントを支援し、長期的な管理を可能にする方法につても述べていく。ハブが監視／監査／制御を提供する範囲は、それぞれのIoTソリューションや、エンタープライズ構造、アーキテクチャの実装方式により、異なるものとなる。

This section presents a high-level Hub architecture design as a reference model for Enterprise IoT managers. Cyber security principles are the foundation of this work, in particular the DCMS "Secure by Design Report" section 4.5 [ref 7] and the IoTSF's "Application Note: Mapping the IoT Security Fundation's Compuliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT" [ref 8]. Supporting these principles and enabling easy implementation and control is a primary aim of the Hub architecture which provides a device management point.

このセクションで説明するのは、ハイ・レベルのハブ・アーキテクチャ・デザインであり、エンタープライズIoTマネージャーが参照するモデルとなるものだ。サイバー・セキュリティの原則は、この作業の基盤である。とりわけ、DCMSの"Secure by Design Report" section 4.5 [ref 7]と、IoTSFの"Application Note: Mapping the IoT Security Fundation's Compuliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT" [ref 8] は重要だ。これらの原則をサポートし、容易な実装と制御を実現することが、デバイスの管理ポイントを提供していくハブ・アーキテクチャの、主たる目的となる。

We do not prescribe or presume certain protocols or solutions, but some reasonable assumptions have been made about number of connected devices, their physical constraints and the "character" of such devices and networks (e.g. if one person sets up the network, or many people have admin rights for different parts of the system). This technology-agnostic approach enables the blueprint to be applicable to a wide-range of systems with such constraints.

特定のプロトコルやソリューションを規定／推定することはないが、接続されているデバイスの数や、それらの物理的制約、デバイスとネットワークの特性については、いくつかの合理的な仮定がなされている（たとえば、1人がネットワークをセットアップする場合や、多くの人々が システム上の各所で管理者権限を持つ場合など）。このアプローチはテクノロジーに捉われないため、制約を持つ各種のシステムのための青写真となる。

3.1 Example of Hub-Based Architecture

The Hub architecture is elaborated here through five elements. The first is a visualization of the Hub architecture and illustrates how the Hub is connected to other devices and security features on the network

ここでは、5つの章を介して、ハブ・アーキテクチャを詳しく説明していく。この1つ目は、ハブ・アーキテクチャの視覚化であり、ネットワーク上のデバイスやセキュリティ機能に対して、どのようにハブが接続されるのかを示していく。

3.1.1 Visualization of Hub-Based Architecture

This is followed by three key processes and their security considerations identified for IoT solution implementation and management, consisting of:

この視覚化は、IoTソリューションの実装／管理のために特定された3つの主要なプロセスと、それらのセキュリティに関する考慮事項を伴う。

- Network Management and Security Tools
- Connecting Devices
- Lifecycle Management

- ネットワーク管理とセキュリティ・ツール
- デバイスの接続
- ライフサイクル管理

Lastly, there are security considerations for the Hub itself (section 3.5 Hub Device Security), including device and software security.

最後に、デバイスとソフトウェアのセキュリティを含む、ハブ自体のセキュリティに関する考慮事項がある (section 3.5 Hub Device Security)。

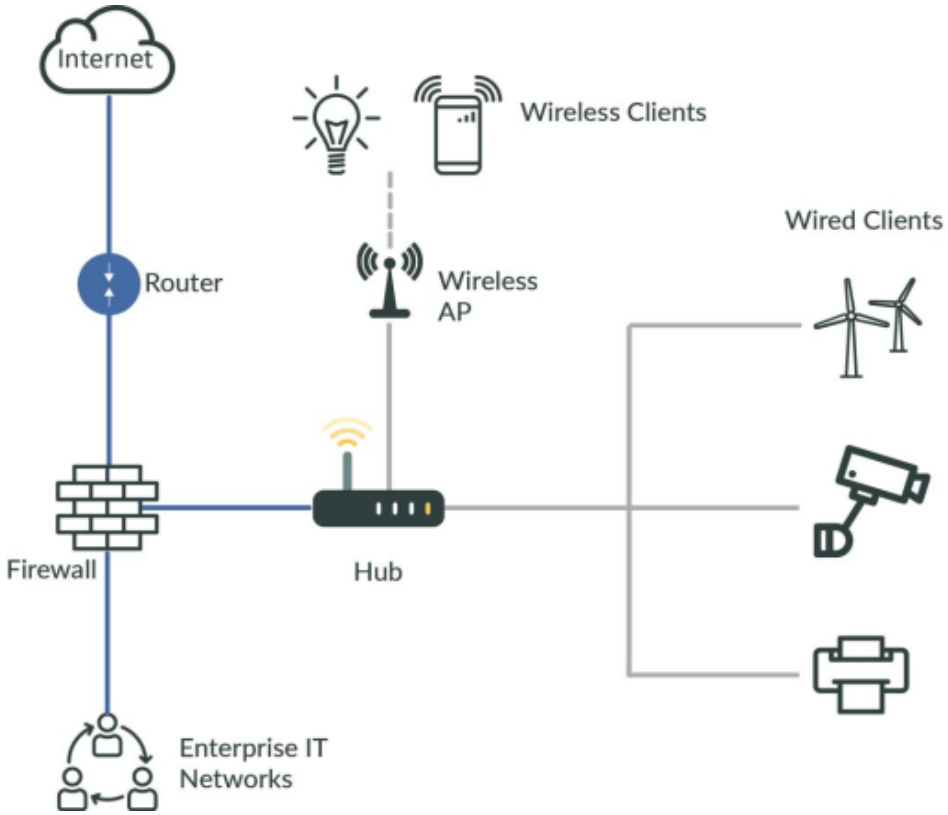

Figure 1: Example Hub Architecture

The visualization in **Figure 1** above shows the multi-layered communication structure within an Enterprise IoT environment, and reflects the complex communication structure between devices, networks and the centralHub. The functions of the router and firewall are shown separately but could also be incorporated into the Hub for Hubs intended for smaller Enterprises. The **local IoT network** (grey lines) is dedicated to IoT devices and separated from the Enterprises' business operations network. **Devices** (grey lines) use this network to talk between themselves, to the Hub and possibly with external elements via a Hub gateway. **The Hub** is at the centre of the IoT ecosystem as it aggregates information and communicates with other architectural elements such as devices and local networks. At the same time, the Hub can act via its connection to the firewall (blue line) as a gateway to external or Enterprise networks as needed.

上記の Figure 1 における視覚化は、エンタープライズIoT環境内の多層化されたコミュニケーション構造を示しており、また、複雑に接続されるデバイス／ネットワーク／セントラル・ハブを反映している。ルーターとファイアウォールの機能は別々に示されているが、小規模企業向けの環境では、ハブのためのハブに組み込むこともできる。ローカルIoTネットワーク（灰色の線）はIoTデバイス専用であり、エンタープライズITネットワークから分離されている。それぞれのデバイスは、このローカルIoTネットワーク（灰色の線）を介して、他のデバイスやハブと、また、場合によってはハブ・ゲートウェイを介して外部要素と通信する。ハブはIoTエコシステムの中心に位置し、情報の集約を行い、他のデバイスやローカル・ネットワークなどのアーキテクチャ要素と通信する。同時に、このハブは、必要に応じてファイアウォールへの接続し（青い線）、外部ネットワークまたはエンタープライズ・ネットワークへのゲートウェイとして機能する。

3.1.2 Reading the Hub-Based Reference Architecture

The Hub-based reference architecture differs from most architectures in that it includes recommendations on the architecture and ideal Hub attributes. For this purpose, we are including a guide on how to read the architecture.

このHub-basedのリファレンス・アーキテクチャは、理想的なハブ属性に関するアーキテクチャ上の推奨事項が含まれているという点で、大半のアーキテクチャとは異なるものとなる。そのため、このアーキテクチャの読み方に関するガイドも含むことにした。

Architecture elements (i.e. Local IoT Network) are categorized under one of the key processes (i.e. Network Management and Security) for managing IoT security. Each architectural element includes three sections:

アーキテクチャの各要素（つまり、ローカルIoTネットワーク）は、IoTセキュリティを管理するための主要なプロセス（つまり、ネットワーク管理とセキュリティ）の1つとして分類される。それぞれのアーキテクチャ要素には、次の3つのセクションがある。

- Introduction to the topic (i.e. Local IoT Network)
- Architecture recommendations
- Hub Attributes

- トピックのイントロダクション(i.e. Local IoT Network)
- 推奨アーキテクチャ
- ハブの属性

The **introduction** provides a brief overview of the topic and its relevance to the Hub architecture. This is targeted at a broad reader audience to provide background and context to the recommendations and attributes.

イントロダクションでは、トピックの概要とハブアーキテクチャとの関連性について説明する。ここでの対象読者は幅広く設定されており、推奨事項と属性に関する背景とコンテキストを提供する。

The **architecture recommendations** provide detail of good and best practices that should be implemented when adopting the Hub architecture, but are not focused on the capabilities of the Hub device.

推奨アーキテクチャでは、このハブ・アーキテクチャを適用するときに実装すべきベスト・プラクティスの詳細を提供するが、対象となるハブ・デバイスの機能には焦点を当てない。

The listed **Hub attributes** provide detail about what is required of the Hub device to support the overall architecture– a key and unique element of the Hub-based architecture.

ハブ属性のリストは、このハブ・デバイスがアーキテクチャ全体をサポートするために必要となる、それぞれの要素の詳細を提供する。つまり、このHub-basedアーキテクチャにおける重要かつ固有の要素となる。

An “Examples” section is also included for each of the three key processes. These are real-world examples of how the architectural elements described in that section can be implemented.

それぞれの、3つの主要プロセスに関する、Examplesセクションも含まれている。それらは、各セクションで説明されるアーキテクチャ要素を、実装する方法の具体的な例である。

3.2 Network Management and Security

3.2.1 Local IoT Network

Enterprises function in a variety of network settings. Some Enterprises may share networks with other organizations, have one or many multiple networks, and may have varying degrees of external network connections such as for cloud computing. For this architecture, it is considered best practice to have one dedicated local network for IoT devices. This is called the “local IoT network” and is considered to offer an extra layer of security to both the devices and Enterprise via separation of IoT device functions from the Enterprise business network in case of a security breach or malfunction.

それぞれの企業は、さまざまなネットワーク設定の中で機能する。たとえば、他の組織とネットワークを共有し、また、1つまたは複数のネットワークを持ち、クラウド・コンピューティングなどの外部ネットワーク接続を用いる企業もある。このアーキテクチャでは、IoTデバイス専用の単一のローカル・ネットワークを持つことが、ベスト・プラクティスと見なされる。これはローカルIoTネットワークと呼ばれ、デバイスとエンタープライズの両方に追加のセキュリティ・レイヤーを提供することで、セキュリティ違反や誤動作が発生した場合に、エンタープライズ・ビジネス・ネットワークからIoTデバイス機能を分離するものと考えられている。

The recommendations provided below are in order of increasing security, but not necessity. Enterprise IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。ただし、最も望ましいハブ機能を特定する際には、エンタープライズIoTアーキテクチャや、リスクの評価、セキュリティ要件などを、考慮する必要がある。

3.2.1.1 Architecture Recommendations

- The local IoT network should create an environment dedicated to IoT devices and communications
- The local IoT network should be separate from the “business” network (local or not)
- Enterprises that share networks with other organizations may consider implementing a new dedicated network, or partitioning their current network
- IoT devices should be networked in a way that ensures devices only communicate with the services and peers required and reinforces confidentiality, integrity, and accessibility of information and networks

- ローカルIoTネットワークは、IoTデバイスと通信のための専用の環境を作成する必要がある。
- ローカルIoTネットワークは、ビジネス・ネットワークから分離される必要がある (local or not)
- 他の組織とネットワークを共有する企業は、新しい専用ネットワークの実装、または、既存ネットワークの分割を検討を行うだろう。
- IoTデバイスをネットワーク化するときには、それらのデバイスが必要とするサービスやピアとのみ通信し、情報およびネットワークの機密性／完全性／アクセス性を強化する必要がある。

3.2.1.2 Hub Attributes

- The Hub should act as a gateway between the IoT network and other networks
- The Hub should minimize the attack surface, identify and address threat vectors

- このハブは、IoTネットワークと他のネットワーク間での、ゲートウェイとして機能する必要がある。
- このハブは、攻撃対象領域を最小限に抑え、脅威ベクターに対する特定／対処を行う必要がある。

3.2.2 Separation of Testing, Staging and Live Systems

Before connecting a new IoT device to the local network, an Enterprise may consider testing the device in a closed staging or test network to verify the device and reduce the risk of the new IoT device or devices, lowering the security of the current IoT ecosystem.

新しいIoTデバイスをローカルネットワークに接続する前に、エンタープライズが検討するのは、クローズド・ステージングまたはテスト・ネットワークでデバイスをテストし、新しいIoTデバイスによるリスクを軽減することで、現状のIoTエコシステムのセキュリティに関する問題を抑えるというステップだろう。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise’s IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 ただし、最も望ましいハブ機能を特定する際には、エンタープライズのIoTアーキテクチャや、リスク評価、セキュリティ要件などを考慮する必要がある。

3.2.2.1 Architecture Recommendations

- The Enterprise should have the ability to connect and test devices before putting them on the live system
- The Enterprise should have at minimum a “test” or “staging” and “live” system
- The Enterprise may decide to have a “development” system if required

- エンタープライズは、デバイスを運用システム上に配置する前に、デバイスを接続してテストする機能を備える必要がある。
- エンタープライズには、少なくとも、テストまたはステージングおよびライブのためのシステム必要とする。
- エンタープライズは、必要に応じて、デプロイメント・システムの導入を判断する場合がある。

3.2.2.2 Hub Attributes

- The Hub should have a test or staging system function
- The Hub should have the ability to manage device setup
- The Hub should manage device connection

- 対象となるハブは、テストまたはステージングのシステム機能を必要とする。
- 対象となるハブは、デバイス・セットアップを管理する能力を必要とする。
- 対象となるハブは、デバイス接続を管理する必要がある。

3.2.3 Gateways and Firewalls

A gateway is a hardware device that acts as a “gate” between two networks. The gateway function may be incorporated into a router, firewall or other device that controls the ingress and egress of traffic in and out of the network.

ゲートウェイは、2つのネットワーク間のゲートとして機能する、ハードウェア・デバイスのことである。ネットワークに出入りするトラフィックを制御するルーター／ファイアウォールなどのデバイスに、このゲートウェイの機能を組み込むことができる。

By it acting as a “gate” between two networks it is considered to be inevitably at the edge of a network, given that all the external network traffic must pass through it. Apart from acting as a gate it may also translate connections from the external network into protocols compatible with those supported by devices within the internal network.

このゲートは、2つのネットワーク間の出入り口として機能する。そして、すべての外部ネットワーク・トラフィックが、ここを通過する必要があることが前提となるため、必然的にネットワーク上のエッジになると見なされる。また、ゲートとして機能するほかに、外部ネットワークのプロトコルを、内部ネットワーク内のデバイスがサポートするプロトコルと、互換性のあるかたちにに変換することもできる。

A firewall is a more advanced type of gateway, which inspects and filters inbound and outbound network traffic and where necessary preventing connections being made with suspicious or unauthorized sources. A further evolution of the firewall that allows application layer (seven) filtering which allows the URL level traffic filtering.

ファイアウォールは、より高度なタイプのゲートウェイである。インバウンドおよびアウトバウンドのネットワーク・トラフィックの検査とフィルタリング行い、疑わしいソースまたは不正なソースとの接続を必要に応じて阻止する。さらに進化したファイアウォールは、URLレベルのトラフィック・フィルタリングを可能にする、アプリケーション層(layer 7)フィルタリングを可能にする。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 ただし、最も望ましいハブ機能を特定する際には、エンタープライズのIoTアーキテクチャや、リスク評価、セキュリティ要件などを考慮する必要がある。

3.2.3.1 Architecture Recommendations

- The Enterprise should implement best practice network security using firewalls and gateways to protect networks and data flows
- The Enterprise should enable traffic segmentation and routing
- The Enterprise should enable traffic monitoring

- エンタープライズは、ネットワークとデータフローを保護するために、ファイアウォールとゲートウェイを活用するベスト・プラクティスのネットワーク・セキュリティを実装する必要がある。
- エンタープライズは、トラフィックのセグメンテーションとルーティングを実現する必要がある。
- エンタープライズは、トラフィックのモニタリングを実現する必要がある。

3.2.3.2 Hub Attributes

- The Hub should act as a gateway to other local and/or external networks
- The Hub should act as a central point for monitoring gateways and firewalls
- The Hub should offer alert and notification in the event of anomalies

- このハブは、他のローカル・ネットワークや外部ネットワークへのゲートウェイとして機能する必要がある。
- このハブは、ゲートウェイとファイアウォールを監視するための中心点として機能する必要がある。
- このハブは、異常が発生した場合に、アラートとノーティフィケーションを提供する必要がある。

3.2.4 Examples of Network Management Tools

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support network management in the IoT ecosystem.

このアーキテクチャは、特定のソリューションを規定するものではなく、また、エンタープライズのIoTセキュリティ要件について仮定するものでもない。したがって、以下の例は、ハブ・アーキテクチャがIoTエコシステムのネットワーク管理に対して、どのようにインターフェースを持ち、どのようにサポートするかを示すものとなる。

- A router (or a Hub) in the Enterprise may be used to split the local network into two – one to function as a "business network" and the other as an "IoT network"
- The Hub can then act as a gateway between the business and IoT networks. For instance, to auto-update shipping logs for manufactured goods
- The IoT manager can use the Hub to further separate the IoT network into "testing" and "live" systems to set up new IoT devices before introducing them to the IoT ecosystem. For instance, for testing interoperability when introducing a new smart lightbulb make or model into the Enterprise environment

- エンタープライズ内のルーター（またはハブ）を用いて、ローカル・ネットワークを2つに分割できる。1つはビジネス・ネットワークとして機能し、もう1つはIoTネットワークとして機能する。

- このハブは、ビジネス・ネットワークとIoTネットワーク間のゲートウェイとして機能できる。たとえば、製造されれた商品の出荷ログの、自動更新などに対応できる。

- IoTマネージャーは、このハブを用いて、IoTネットワークをテスト・システムとライブ・システムに分離し、IoTエコシステムに導入する前の、新しいIoTデバイスをセット・アップすることができる。たとえば、新しいモデルのスマート電球を、エンタープライズ環境に導入する際の相互運用性のテストなどに活用できる。

3.3 Connecting Devices Securely

3.3.1 Authentication and Authorization

The secure authentication of an IoT device's identity and its software deployed in the Enterprise is critical to ensuring that only approved and trusted devices are deployed into the Enterprise. Authentication is the process of verifying that a thing (or person) is what it claims to be. Authenticating a device verifies its identity and/or attributes of the device. Once authenticated, the network manager can authorize the device to function on the network.

IoTデバイスのID安全な認証と、エンタープライズ内にディプロイされたソフトウェアの安全な認証は、承認／信頼されたデバイスのみがエンタープライズ内にディプロイされることを保証する、きわめて重要な事項となる。認証とは、物や人が主張する何かを確認するプロセスである。デバイスを認証することは、そのデバイスのIDや属性を検証することである。そして、認証が完了すると、ネットワーク管理者は、そのデバイスがネットワーク上で機能することを承認できる。

Authentication supports other good security practices such as authorization and non-repudiation. Non-repudiation is "the ability to prove that a person, entity or process cannot deny having carried out an action" [ref 9]. Authorization grants permissions to the devide, such as network access and associated parameters. In the same vein, permissions can be taken away from specific devices, for instance at end-of-life or in the event of ownership transfer.

認証がサポートする優れたセキュリティ・プラクティスとして、承認および否認の防止などが挙げられる。否認の防止とは、個人／団体／プロセスが実施したアクションを、否定できないことを証明する能力のことである [ref 9]。承認がデバイスに与える権限には、ネットワークへのアクセスや、パラメータの設定などがある。同様に、特定のデバイスの寿命が尽きたときや、そのデバイスの所有権が譲渡された場合には、それらの権限を奪うことができる。

In order for successful authentication and authorization in a mixed-vendor environment (i.e. for the Enterprise to not be constrained by vendor or ecosystem lock-in) devices need to be interoperable and support internationally recognized standards. Whilst standardization is still in its infancy, there are initiatives in this area, an example is the IETF draft on the remote bootstrapping of PKI credentials [ref 17]. Solving issues of interoperability is not a primary aim of this document, but should be a key consideration for OEMs developing devices for the Enterprise and for IoT managers and developers implementing these hub architectures. Particular areas that need standardization are:

複数のベンダーが混在する環境において、認証と承認を成功させるためには（ベンダーやエコシステムのロックイン制約から逃れるためには）、デバイスの相互運用を可能にする必要がある、また、国際的に認められた標準をサポートする必要がある。標準化は始まったばかりだが、この分野にはイニシアチブが登場している。たとえば、PKI資格情報のリモート・ブートストラップに関しれは、IETFドラフトがある [ref 17]。このドキュメントにおいて、相互運用性の問題を解決することは、主な目的ではない。しかし、エンタープライズ向けのデバイスを開発するOEMや、ハブ・アーキテクチャを実装するIoTマネージャーや開発者にとって、それらは重要事項となる。 標準化が必要な特定の領域は、次のとおりとなる。

- Protocol or protocols for IoT devices and hubs which support:
  - Trusted software update which allows the option of a Hub to act as a broker between manufacturer and device, particularly within a heterogeneous environment of multiple manufacturers and their devices
  - IoT device secure credential dissemination which can be authenticated by the Hub or Hubs.
  - A Hub being able to enumerate IoT devices and establish their state in a safe and secure way.
- A common method of describing detected security events acting on an IoT device

- IoTデバイスおよびハブがサポートする、単一もしくは複数のプロトコル:
  - ハブのオプションが、メーカーとデバイス間のブローカーとして機能することを可能にする、信頼できるソフトウェア・アップデート。とりわけ、複数のメーカーと、複数のデバイスが混在する、異種環境において重要。
  - 単一または複数のハブで認証が可能な、IoTデバイスの安全資格情報の配布。
  - 安全かつ確実な方法で、バブによりIoTデバイスを列挙する能力と、IoTデバイスのステートを確立する能力。
- IoTデバイスに対して作用する、検出されたセキュリティ・イベントを記述する、共通のメソッド。

Unlike traditional IT equipment which either has a human interface or a standards-based interface used to configure and load trust credential, IoT devices are typically "headless". As a result, the installation of the trust credentials to allow the device(s) and the Enterprises' network to authenticate each other represent a challenge to scalable deployment. In the case of network access this can be problematic for Enterprises when a device expects its wireless configuration to be carried out over a local wireless interface and involves the sharing of the Enterprise's wireless credentials to the device.

従来からのIT機器は、信頼できる資格情報のコンフィグレーションとロードに用いる、ヒューマン・インターフェイスまたは標準ベースのインターフェイスを備えているが、通常のIoTデバイスは headless である。その結果、デバイスとエンタープライズのネットワークが相互に認証できるようにするための、信頼できる資格情報のインストールにおいて、スケーラブルなデプロイメントは課題を残している。ネットワーク・アクセスの場合において、対象となるデバイスのワイヤレス・コンフィグレーションが、ローカル・ワイヤレス・インターフェイスを介して実行されることを期待し、そのデバイスに対するエンタープライズ・ワイヤレス資格情報の共有を伴う場合には、問題が生じるかもしれない。

Throughout the lifecycle of an IoT device, authentication and authorization will be used repeatedly to verify and manage devices, including assigning and revoking privileges. Authentication and authorization form a foundation for additional security layers such as (in order of increasing security, but not necessity):

IoTデバイスのライフサイクル全体を通じて、デバイスの検証／管理のために、認証と承認は繰り返し使用されるが、そこには特権の割当てと取消しも含まれる。認証と承認は、以下のような追加のセキュリティ・レイヤー基盤を形成する（セキュリティ強化のためであり、必須ではない）。

- **Device Identity Management** – the ability to identify a device or group of devices, enabling actions such as authorization and privilege management
- **Black or Whitelisting** – verifying only desired (e.g. authenticated) devices access the network by managing access or privilege control tools (e.g. granting authorization)
- **Granting Privileges** – authorizing access or actions based on attributes (e.g. allowing devices connected to a "visitor network" access to a "visitor printer", but not the Enterprise business network)
- **Revoking Privileges** – removing or preventing a privilege based on attributes (i.e. removing authorization to access the Hub system from a decommissions smart light solution which is installed in the building but no longer in use)
- **Roots of Trust** – use of trust-building tools, such as certificates or encryption, to provide a trust foundation in the IoT system (e.g. using certificate authorities to authenticate devices)
- **Validating Software Updates** – with the use of digital signatures and/or encryption based upon a suitable root of trust to validate that the software update is from an authentic source, typically the product's OEM or authorized software provider

- **Device Identity Management** – デバイスまたはデバイスのグループを識別し、承認や特権管理などのアクションを可能にする機能。
- **Black or Whitelisting** – アクセスや特権を制御するツール（承認の付与など）を管理することで、望ましい（認証済など）デバイスのみが、ネットワークにアクセスすることを確認する。
- **Granting Privileges** – 属性に基づいて、アクセスまたはアクションを承認する（たとえば、ビジター・ネットワークに接続されているデバイスに対して、ビジター・プリンターへのアクセスを許可するが、エンタープライズ・ビジネスネットワークへのアクセスは許可しない）。
- **Revoking Privileges** – 属性に基づいて、特権を削除／停止する（たとえば、建物には設置されているが使用されなくなった、廃棄されるべきスマート・ライト・ソリューションから、ハブ・システムにアクセスするための承認を削除する）。
- **Roots of Trust** – 証明書や暗号化などの信頼構築ツールを用いて、IoTシステムに信頼の基盤を提供する（たとえば、認証局を用いたデバイスの認証）。
- **Validating Software Updates** – 適切なトラスト・ルーツに基づくデジタル署名や暗号化を用いて、ソフトウェアの更新が本物のソースからのものであることを検証する（通常は製品のOEMまたは認定ソフトウェア・プロバイダー）。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 ただし、最も望ましいハブ機能を特定する際には、エンタープライズのIoTアーキテクチャや、リスク評価、セキュリティ要件などを考慮する必要がある。

3.3.1.1 Architecture Recommendation

- Enterprises should use only IoT solutions that can be authenticated where possible to ensure only known devices are allowed on the network and support ongoing trust between devices
- Develop authorization management structure to determine a device's privileges on the network (i.e. connectivity, routing, requests, files)
- Have the ability to revoke authentication and/or authorization to decommission devices or transfer ownership

- エンタープライズは、認証が可能なIoTソリューションのみを用いて、既知のデバイスのみがネットワーク上で許可されていることを確認した上で、デバイス間の継続的な信頼をサポートする必要がある。
- ネットワーク上のデバイスの特権（接続／ルーティング／リクエスト／ファイルなど）を決定するための、承認管理構造を開発する。
- 認証や承認の取消によるデバイスの廃や、所有権を譲渡するための機能を持つ。

3.3.1.2 Hub Attributes

- The Hub should be a central point for supporting authentication. It may:
  - Carry out authentication processes
  - Act as a cache for authenticated devices
  - Store authentication credentials
  - Support varying levels of authentication (e.g. single token, server, and mutual authentication)
- The Hub should be a central point for supporting authorization. It may:
  - Act as a device management tool to apply or revoke privileges
  - Support creation and enforcement of permissions lists (e.g. black- and whitelists)
  - Support trusted device/group identity management
- The Hub should provide alerts if an authenticated device has been tampered, authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in password and cryptography systems to support authentication and authorization processes

- ハブは、認証をサポートするための中心点である必要がある。以下を可能にする：
  - 認証プロセスを実行する
  - 認証されたデバイスのキャッシュとして機能する
  - 認証資格情報を保存する
  - 多様な認証レベルをサポートする（シングル・トークン、サーバー、相互認証など）
- ハブは、承認をサポートするための中心点である必要がある。以下を可能にする：
  - 特権の適用／取消を行うためのデバイス管理ツールとして機能する
  - 権限リストの作成／実施をサポートする (たとえば black- and whitelists)
  - 信頼できるデバイス／グループのID管理をサポートする
- 認証されたデバイスが改ざんされた場合や、認証特権が変更された場合、そして、不正なアクションを実行しようとしている場合に、ハブはアラートを提供する必要がある。
- ハブは、認証／承認プロセスをサポートするために、パスワードおよび暗号化システムにおいて、少なくともベスト・プラクティスを使用する必要がある。

3.3.2 Secure Boot

Secure boot is the process through which the device validates the integrity of the software from boot time onwards. For larger systems there are three levels of secure boot types in increasing level of security listed below:

セキュア・ブートとは、デバイスがブートされた後に、ソフトウェアの整合性が検証されるプロセスのことである。大規模なシステムの場合には、セキュリティのレベルを上げるために、以下に示す3つのレベルのセキュア・ブート・タイプが存在する。

- **Secure Boot**: The device verifies that its bootloader is correctly digitally signed and that no changes have been made to the firmware
- **Trusted Boot**: The device's bootloader checks the digital signature of the operating system and the operating system checks the integrity of every component of the startup process before loading it
- **Measured Boot**: The device's firmware logs the boot process metrics including the Operating System boot and securely sends the metrics to a trusted server that can attest to the trustworthiness of the device

- **Secure Boot**: デバイスにより、ブートローダーが正しくデジタル署名され、ファームウェアに変更が加えられていないことが確認される
- **Trusted Boot**: デバイスのブートローダーにより、オペレーティング・システムのデジタル署名がチェックされ、オペレーティング・システムによりロードが実行される前に。スタートアップ・プロセスのすべてのコンポーネントの整合性がチェックされる
- **Measured Boot**: デバイスのファームウェアが、オペレーティングシステムの起動を含めた、ブート・プロセスのメトリックをログに記録する。続いて、デバイスの信頼性を証明するトラスト・サーバーへ向けて、それらのメトリックが安全に送信される

In smaller embedded systems, the Secure Boot and Trusted Boot may involve the use of a microcontroller or microprocessor that starts executing software from internal and immutable memory. The software stored in the immutable memory in the microcontroller is considered inherently trusted (i.e., the root of trust) because it cannot be modified. This inherently trusted software then authenticates the software, such as the operating system not stored in immutable memory, through a cryptographic process such as digital signing or decryption, using a root of trust stored securely within the microcontroller/processor.

小規模な組み込みシステムのセキュア・ブートとトラステッド・ブートの場合には、内部メモリと不変メモリからソフトウェアの実行を開始する、マイクロコントローラやマイクロプロセッサの使用が含まれることがある。マイクロ・コントローラの不変メモリに保存されているソフトウェアは、変更できないため、本質的に信頼されると考えられる（つまり、信頼のルート）。続いて、この本質的に信頼できるソフトウェアにより、ソフトウェアの認証が行われる。その対象としては、暗号化プロセスを通じて認証される不変メモリ以外に保存されたオペレーティング・システムや、マイクロコントローラ／プロセッサ内に安全に保存された信頼のルートを使用して認証されるデジタル署名や復号化などがある。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 ただし、最も望ましいハブ機能を特定する際には、エンタープライズのIoTアーキテクチャや、リスク評価、セキュリティ要件などを考慮する必要がある。

3.3.2.1 Architecture Recommendations

- Use only Hub solutions that support secure boot to ensure that their integrity cannot be compromised and that only authorized software can be deployed onto them
- Have the ability to revoke authentication and/or authorization to enable the secure decommissioning of Hubs or transfer Hub ownership

- ハブ・ソリューションのみを用いて、整合性が損なわれないセキュア・ブートと、承認されたソフトウェアのみのデプロイをサポートする。
- 認証や承認を取り消す能力を持つことで、ハブの安全な廃止や、ハブの所有権の譲渡などを実現する。

3.3.2.2 Hub Attributes

- The Hub should provide alerts if an attempt is made to install unauthenticated software or the Hub has been tampered, authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in roots of trust and sources of entropy, for its cryptography systems to ensure support for secure authentication and authorization processes. For further details on this best practice subject please see in the "IoT Security Compliance Framework section" [ref 1]

- ハブはアラートを提供することで、認証されていないソフトウェアのインストールを通知しなければならない。同様に、ハブが改ざんされた場合や、認証権限が変更された場合、不正なアクションが実行される場合には、アラートを提供する必要がある。
- ハブは、信頼のルートとエントロピーのソースで少なくともベスト・プラクティスを用いて、暗号化システムによる認証／承認のプロセスの安全なサポートを確実にする必要がある。ここで言うベスト・プラクティスの詳細については、IoT Security Compliance Framework section [ref 1] を参照のこと。

3.3.3 Roots of Trust

Roots of trust are at the core of this Hub-based architecture because the Hub acts as a central trust anchor and management tool, deciding which devices or network infrastructure to trust. Without a root of trust, particularly public roots of trust, this is a difficult problem to solve. Public roots of trust are considered a more secure and practical solution than private roots of trust in the Enterprise context, primarily because of the increased responsibility placed on the Enterprise and risks that come with poor management of private roots of trust. Public roots of trust also better support other needs such as interoperability.

このHub-basedのアーキテクチャの中核に信頼のルートはあるのは、このハブがトラスト・アンカーおよび管理ツールの中心として機能するからであり、それにより、信頼できるデバイスやネットワーク・インフラストラクチャが決定される。信頼のルートを持たずに、とりわけ、信頼のパブリックなルートを持たずに、問題を解決することは困難である。信頼のパブリック・ルーツは、エンタープライズにおける信頼のプライベート・ルーツと比較して、より安全で実用的なソリューションと見なされる。その主たる理由は、企業に課せられる責任が増大している状況と、信頼のプライベート・ルーツにおける、不十分な管理に伴うリスクが増大している状況にある。信頼のパブリック・ルーツは、相互運用性などのニーズに対しても、より適切なサポートを提供する。

Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. By design, roots of trust must be highly secure since they are used as a fundamental trust point. To prevent tampering or extraction of their contents, roots of trust are normally implemented in hardware to provide a strong trust foundation.

信頼のルーツは、信頼性の高いハードウェア／ファームウェア／ソフトウェアにより構成され、特定かつ重要なセキュリティ機能を実行する。設計上、信頼のルートは、基本的な信頼のポイントとして使用されるため、高度かつ安全でなければならない。信頼のルートは通常、コンテンツの改ざんや漏えいを防ぐために、ハードウェアに実装され、強力な信頼の基盤を提供する。

An Enterprise will need to make an informed decision on whether best to use public or private roots of trust for its specific IoT deployment model. While there might be certain situations where private roots are preferable as discussed below, in general private roots of trust are not considered the most effective solution in the context of Enterprise IoT. Implementing a private root of trust places additional responsibility on the Enterprise to ensure roots of trust are managed appropriately.

エンタープライズにおいては、そのIoTデプロイメント・モデルに対して、最善のパブリック／プライベート信頼ルートを適用するために、十分な情報に基づく判断をくだす必要がある。以下で説明するように、プライベート・ルートが望ましい状況があるかもしれないが、一般的なプライベート・ルートの信頼度は、エンタープライズIoTのコンテキストにおいて、最も効果的なソリューションとは見なされていない。プライベートの信頼ルートを実装すると、信頼のルートを適切に管理すべきという責任が、エンタープライズに課せられるようになる。

Executing key management and creating private roots of trust can result in interoperability issues and security weaknesses. For instance, private roots of trust used to embed certificates in devices may result in issues of management and scalability – particularly where devices may have limited or no user interface (“headless devices”). Keys left unmanaged, certificates not revoked appropriately, or not re-issued to keep pace with technological change can weaken security and negatively impact trust in the IoT ecosystem.

信頼のプライベート・ルートを作成し、キー管理を実施すると、相互運用性に問題を生じ、また、セキュリティ面で弱点が生じる可能性がある。たとえば、デバイスに証明書を埋め込むために用いる信頼のプライベート・ルートは、とりわけデバイスのユーザーインターフェイスが制限されている場合や、ユーザーインターフェイスが存在しない場合に（headless）、管理とスケーラビリティの問題を引き起こす可能性がある。それ以外にも、不適切なキー管理が実施されている場合や、証明書が適切に取り消されていない場合、技術の変化に対応するためにキーが再発行されていない場合において、セキュリティが弱体化することでIoTエコシステムの信頼性に悪影響を与える可能性がある。

Private roots of trust do have specific benefits in the case of internal services authentication, for example authenticating connections into the Enterprise’s internal WiFi or virtual private network(s) (VPN). These are cases where there are significant benefits to the Enterprise being able to specifically control which devices or connections can be authenticated by internal systems. If the Enterprise uses it own private root then no other entity can issue certificates except those authorized within the Enterprise and the certificate profiles can be customised to suit the Enterprise’s specific requirements.

信頼のプライベート・ルートを用いると、たとえば、エンタープライズ内のWiFi／VPNへの認証接続などで、メリットが生じることがある。内部システムにより認証が可能なデバイス／コネクションを、明確に制御できるエンタープライズであれば、大きなメリットになるだろう。ただし、エンタープライズが独自のプライベート・ルートを用いる場合には、エンタープライズ内で承認されたエンティティを除いて、他のエンティティは証明書を発行でなくなる。そして、証明書のプロファイルは、エンタープライズにおける特定の要件に合わせてカスタマイズされるだろう。

As their name implies, public roots of trust are ones which are publicly accessible and allow third parties to authenticate each other without prior credential exchange. Embedding public roots of trust where possible helps circumvent issues presented by private roots – such as scalability – and supports a long-term approach to treating risks associated with Enterprise IoT deployments. A number of the challenges of the deployment of roots of trust can be overcome with a combination of the use of public roots of trust and the use of Identity Access Management systems.

その名前が示すように、信頼のパブリック・ルートは、パブリックなアクセスが可能であり、また、資格情報を事前に交換しなくても、サードパーティ同士が相互に認証できるようになる。信頼のパブリック・ルートの組み込みが可能ならば、プライベート・ルートが引き起こすスケーラビリティなどの問題が回避され、エンタープライズIoTデプロイメントにおけるリスク処理を推進するための、長期的なアプローチがサポートされるだろう。信頼ルートの展開に関する数多くの課題は、信頼のパブリック・ルートの利用と、IDアクセス管理システムの利用を、組み合わせることで克服できる。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 ただし、最も望ましいハブ機能を特定する際には、エンタープライズのIoTアーキテクチャや、リスク評価、セキュリティ要件などを考慮する必要がある。

3.3.3.1 Architecture Recommendations

- If considering private roots of trust, the Enterprise should execute a risk assessment to help identify the best way forward
- Implementations should support best practices in roots of trust [see refs 3, 12 and 16]
- Roots of trust should be utilized to support authentication and authorization processes
- Roots of trust may be used to support identification of malicious software

- 信頼のプライベート・ルーツを検討する場合、エンタープライズはリスク評価を実施することで、今後における最善の方法を特定しなければならない。
- 信頼のルーツにおいては、実装でベストプラクティスをサポートする必要がある [see refs 3, 12 and 16]
- 認証／承認のプロセスをサポートするための、信頼のルートを活用する必要がある。
- 悪意のソフトウェアの識別をサポートするために、信頼のルーツを活用できるかもしれない。

3.3.3.2 Hub Attributes

- The Hub shall support the cryptographic hashing and encryption/decryption functions used in the authentication of chains of trust, in particular:
  - A Hub shall support industry standards in cryptography
  - A Hub shall support best practices in cryptography [see ref 1]
  - A Hub shall have a hardware root of trust

- このハブは、信頼チェーンの認証で使用される暗号化ハッシュおよび、暗号化／復号化の機能のサポートも提案する。とりわけ、以下のケースで顕著である：
  - あるハブが、暗号化における業界標準のサポートを提案する
  - あるハブが、暗号化のベスト・プラクティス・サポートを提案する[see ref 1]
  - あるハブが、信頼のハードウェア・ルートを提案する

- The Hub should have the ability to manage private and public roots of trust
    - The Hub may be able to create and manage private roots of trust for the Enterprise
    - The Hub should be able to support public roots of trust
    - The Hub should securely store and/or cache roots of trust

- このハブは、信頼のプライベート／パブリック・ルーツを管理する能力を持つべきだ。
    - このハブは、エンタープライズ用の信頼のプライベート・ルートを作成／管理できるだろう。
    - このハブは、信頼のパブリック・ルーツをサポートする能力を持つべきだ。
    - このハブは、信頼のルートを、安全に保存／キャッシュすべきだ。

- The Hub may enable roots of trust by acting as an intermediary between device and certificate authority

- このハブは、デバイスと認証局の仲介役として機能することで、信頼のルートを有効にする能力を持つだろう。

- The Hub should provide a cryptographically secure method to update and revoke its cryptographic keys, including those keys used for the authentication of updates

- このハブは、暗号化キーを更新／取消ための、暗号化された安全な方法を提供する必要がある。そこには、更新の認証に使用されるキーも含まれる。

- The Hub may use roots of trust to assist detection of malicious software

- このハブは、悪意のソフトウェアの検出を支援するために、信頼のルートを使用するかもしれない。

3.3.4 Examples of Tools to Connect Devices Securely

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support connecting devices securely in the IoT ecosystem.

このアーキテクチャは、特定のソリューションを規定することはなく、エンタープライズのIoTセキュリティ要件を仮定するものでもない。IoTエコシステムにおいて、ハブ・アーキテクチャがデバイスを安全に接続／サポートする例を、以下に記す。

- A Hub can manage white lists to ensure only authorized devices connect to the IoT network. For instance, in shared office spaces multiple Enterprises may have access to local networks. However, whitelisting IoT devices allowed onto the IoT network will protect the network from being accessed by office, IoT and BYOD devices in the shared space

- ハブはホワイトリストを管理することで、承認されたデバイスのみがIoTネットワークに接続するよう保証する。たとえば、共有オフィス・スペースにおいては、複数の企業がローカル・ネットワークにアクセスする場合がある。ただし、IoTネットワークで許可されたIoTデバイスのホワイトリストは、共有スペース内のOffice/IoT/BYODデバイスによるネットワークへのアクセスを阻止する。

- A headless device, such a motion sensor, with a root of trust may need to be authenticated by a certificate authority. In this case, the Hub can act as an intermediary, communicating directly with a certificate authority and providing a user interface to prompt or track the authentication process. After the root of trust has been authenticated, the IoT manager can grant the motion sensor authorization to access the IoT network

- たとえば、信頼のルートを持つモーション・センサーなどの headless デバイスは、認証局による認証を必要とする場合がある。この場合において、ハブは仲介者として機能し、認証局とダイレクトに通信し、認証プロセスを導き追跡するためのユーザー・インターフェイスを提供する。信頼のルートが認証された後に、IoTマネージャーはモーション・センサーに対して、IoTネットワークにアクセスするための承認を与えることができる。

3.4 Lifecycle Management

3.4.1 Monitoring and Audit

Monitoring and audit of IoT ecosystem devices, networks, resources, and performance are key elements of IoT security. Information and measures resulting from monitoring and auditing can be aggregated in a centralized location for better IoT ecosystem visibility and control. A Hub acts as a central repository of information for IoT managers about the functioning and statuses of the IoT ecosystem and can be used to inform resulting actions. The IoT manager will be able to take more informed decisions based on what is learned and can be applied via the Hub, particularly with the rapid development of machine learning and data analytics. This includes aggregation of information from other security tools such as firewalls, gateways, and network access controls. These tools may or may not be directly managed from the Hub, however, they may share information such as:

IoTエコシステムのデバイス／ネットワーク／リソース／パフォーマンスに関する監視と監査は、IoTセキュリティの重要な要素である。監視と監査から得られる情報と測定値をセンタライズされた場所に集約し、IoTエコシステムの可視性と制御を向上させることが可能となる。ハブは、IoTマネージャー向けの情報の中央リポジトリとして機能し、IoTエコシステムの機能とステータスに対応することで、結果として生じるアクションを通知する。IoTマネージャーは、ハブを介して学習された内容に基づき、さらには、機械学習とデータ分析の急速な発展により、大量の情報に基づいた意思決定を行うことが可能になるだろう。そこには、ファイアウォール／ゲートウェイ／ネットワーク・アクセス・コントロールなどの、セキュリティ・ツールから集約された情報も含まれる。これらのツールは、ハブからダイレクトに管理される場合と、されない場合があるが、以下のような情報が共有されるだろう。

- **Notifications** – A notification is information delivered by the system to the IoT ecosystem managers and/or IoT users as appropriate. This could include push notifications (such as an unexpected incident alert notification) or pull notifications (such as requested status updates). Notifications support security by providing essential information to the IoT manager on events and incidents in the ecosystem and thus respond appropriately

- **Alerts** - An alert is a type of notification that is important or time sensitive. For instance, alerts can support IoT security via timely notification, and thus response, when incidents are detected in the IoT ecosystem

- **Status Updates** – Status updates are a type of notification that provide the ability for IoT managers to determine the status of an IoT device or network at any given time, such as device status (e.g. on/off, in use/not in use), or software update/ patch status. Status updates support security by contributing to the overall snapshot of IoT ecosystem statuses, health, and security management processes

- **Report** – A report, such as an incident report or system snapshot, can include historic and current information such as time/date stamps, impacted networks and devices, taken or scheduled actions. Reporting provides an understanding of events and may also assist in demonstrating compliance with local and industry-specific regulations

- **Notifications** – ノーティフィケーションとは、IoTエコシステム・マネージャーやIoTユーザーへ向けて、システムから適切に配信される情報のことである。そこには、プッシュ通知（予期しないインシデント・アラートなど）またはプル通知（要求されたステータス更新など）が含まれるだろう。ノーティフィケーションは、エコシステム内のイベント／インシデントに関する重要な情報を、IoTマネージャーに提供することで、適切なセキュリティを実現する。

- **Alerts** - アラートとは、ノーティフィケーションの一種であるが、重要かつ緊急のものとなる。たとえば、アラートは、IoTエコシステム内でインシデントが検出されたときに、タイムリーな通知を行うことで、つまり適切な対応を行うことで、IoTセキュリティをサポートできる。

- **Status Updates** – ステータス・アップデートとは、ノーティフィケーションの一種であるが、任意の時点においてIoTマネージャーが、IoTデバイスやネットワークのステータスを判断するための機能を提供する。そこには、デバイスのステータス（オン／オフや使用中／未使用など）や、ソフトウェアのアップデート／パッチのステータスなどが含まれる。ステータス・アップデートは、IoTエコシステムのステータス／ヘルス／セキュリティ管理プロセスなどの、全体的なスナップショットを提供することでセキュリティをサポートする。

- **Report** – レポートとは、インシデント報告やシステム・スナップショットなどのことであり、タイムスタンプや、影響を受けるネットワーク／デバイス、アクションのスケジュールなどで構成される、履歴および現状の情報を取り込むものとなる。レポートにより、イベントに対する理解が促進され、また、ローカル／スタンダードのコンプライアンスに対する、準拠の実証も促進される。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものでだが、必須ではない。最も望ましいハブ機能を特定する際には、それぞれのエンタープライズにおけるIoTアーキテクチャ／リスク評価／セキュリティ要件を考慮する必要がある。

3.4.1.1 Architecture Recommendations

- An Enterprise should have tools for monitoring and auditing its IoT ecosystem, which supports troubleshooting, checking network health, tracking data flows, and demonstrating policy compliance. This may include:
    - Monitoring/auditing devices
    - Monitoring/auditing networks and Hubs
    - Monitoring/auditing traffic flows
    - Raising alerts and notifications when an event is detected
- An Enterprise should have a central location to review alerts, notifications, or reports resulting from monitoring and audits
- Monitoring and auditing should be provided to the extent needed to manage the network. This may include information such as: ‘
    - Metrics on resource consumption (e.g. power)
    - Data transfer and flows
    - Access requests and logs
    - Changes to device and network parameters
    - Temporary devices and associated actions

- エンタープライズは、IoTエコシステムを監視／監査するためのツールを備える必要がある。それらにより、トラブルシューティング／ネットワーク・ヘルスのチェック／データフローの追跡／ポリシー・コンプライアンスの実証などがサポートされる。具体的には、以下のものが含まれる。
    - デバイス群の監視／監査
    - ネットワークとハブの監視／監査
    - トラフィック・フローの監視／監査
    - イベントが検知されたときのアラートとノーティフィケーションの発出

- エンタープライズは、監視と監査の結果として生じるアラート／ノーティフィケーション／レポートを確認するための、センタライズされた場所を持つ必要がある。

- ネットワークの管理に必要な範囲で、監視／監査を提供する必要がある。具体的には、以下のような情報を含むだろう。
  - o リソース消費に関する指標 (e.g. power)
  - o データの転送とフロー
  - o アクセスのリクエストとログ
  - o デバイスとネットワークのパラメータ変更
  - o テンポラリーなデバイスと、割り当てられたアクション

It is important to note that network monitoring and audit are subject to local policy and regulation – such as privacy and data protection – and should be implemented in a manner consistent with relevant legislation for that Enterprise sector.

ネットワークの監視／監査は、たとえばプライバシーやデータ保護などの、ローカルにおけるポリシーと規制の対象となることに注意する必要がある。また、対象となるエンタープライズ部門における規約と一致する方法で、実装する必要がある。

3.4.1.2 Hub Attributes

- The Hub should enable monitoring and audits. These may be done continuously, be time-constrained or done routinely

- The Hub should provide reporting tools for monitoring and audits, this may include:
  - o A log of monitoring and audit activity
  - o Access to past reports
  - o Query options
- Following monitoring or audit, the Hub should provide alerts or notifications of relevant information such as incidents or measures outside set parameters
- As a result of monitoring and audit, the Hub should enable Enterprise IoT managers to take necessary actions either directly via the Hub or outside the Hub. This may include actions such as:
  - o Controlling traffic flows and segmentation
  - o Implementing anti-virus/malware solutions
  - o Pushing updates or patches to devices
- Hubs supporting roots of trust should be able to audit and update roots as necessary

- ハブは監視／監査を有効にする必要がある。それらは、継続的／定時的／定期的に実行される。

- ハブは、監視／監査のためのレポート・ツールを提供する必要がある。以下のものが含まれるだろう。
  - o 監視／監査のアクティビティを記録するログ。
  - o 過去のレポートへのアクセス。
  - o クエリーのオプション。
- ハブは監視／監査に続いて、インシデントやパラメータの設定違反などの関連情報を、アラートやノーティフィケーションで通知する必要がある。
- ハブは監視／監査の結果として、エンタープライズIoTマネージャーによる、ハブを介したアクションおよび、ハブの外部でのアクションを、実行できるようにする必要がある。具体的には、以下のようなアクションが含まれだろう。
  - o トラフィック・フローをセグメンテーションの制御
  - o アンチウィルス／マルウェア・ソリューションの実装
  - o デバイスに対するアップデートとパッチの実施
- 信頼のルートをサポートするハブは、必要に応じてルートを監査／更新する能力を持つ必要がある。

3.4.2 Update and Patch

A simple but configurable way of securely updating and patching across the IoT ecosystem is an important aspect of IoT security. Updating and patching helps to protect against known threats, fix security vulnerabilities, protect against bugs and improve performance. IoT managers should be able to have a central point of reference for related information such as:

IoTエコシステムを横断するかたちで、アップデート／パッチを安全に適用する方法は、シンプルであってもコンフィグレーションが可能であるため、IoTセキュリティにおける重要な側面となる。アップデート／パッチの適用は、既知の脅威からの保護や、セキュリティ脆弱性の修正、バグからの保護、パフォーマンスの向上に寄与する。IoTマネージャーは、参照のための中心的なポイントを持つことが必要であり、かつ、以下のような関連情報に対処する必要がある。

- Completed Updates
- Scheduled Updates
- Update Source
- Update Verification

- 完了したアップデート
- スケジュールされているアップデート
- アップデートのソース
- アップデートのための検証

Implementing reliable mechanisms for tracking and implementing updates supports the integrity, privacy and security of the IoT ecosystem and helps to enable interoperability.

アップデートを実施／追跡するための、信頼できるメカニズムを実装すると、IoTエコシステムにおける整合性／プライバシー／セキュリティがサポートされ、相互運用性が実現される。

The recommendations provided below are in order of increasing security, but not necessity. Each Enterprise's IoT architecture, risk assessment, and security requirements should be taken into consideration when identifying the most desirable Hub features.

以下に示す推奨事項は、セキュリティを強化するためのものだが、必須ではない。 最も望ましいハブ機能を特定する際には、それぞれのエンタープライズにおける、IoTアーキテクチャ／リスク評価／セキュリティ要件を考慮する必要がある。

3.4.2.1 Architecture Recommendations

- IoT devices should support software and firmware updates and patching from necessary sources (e.g. Enterprise- or manufacturer-pushed)
- The IoT manager should be able to log updates/patches and create related reports
- Update mechanisms should include secure boots and regular reboots for devices, such as code signing to verify updates

- IoTデバイスは、必要なソースに基づいて、ソフトウェアとファームウェアのアップデート／パッチ適用をサポートする必要がある（例：エンタープライズやメーカーがプッシュするもの）。
- IoTマネージャーは、アップデート／パッチをログに記録し、関連するレポートを作成する能力を持つ必要がある。
- アップデート・メカニズムは、更新を確認するためのコード署名などの、デバイスのためのセキュアなブートと定期的なプートを取り込む必要がある。

3.4.2.2 Hub Attributes

- The Hub should keep an update/patch log with reporting capabilities, for example:
  - The Hub should log information regarding past and future updates such as time stamps or scheduled updates
  - The Hub should log information about update provenance and verification
  - The Hub should support automatic and manual input
- The Hub should be able to manage updates and patching centrally to the extent possible, for example:
  - The Hub may be able to cache updates for IoT devices
  - The Hub should support devices with limited or intermittent connectivity and multi-part updates
  - The Hub should support automatic and manual initiation of updates
  - The Hub should be able to manage updates from a variety of sources (e.g. Enterprise- and manufacturer-pushed)
- The Hub itself should be kept as up to date as possible as it provides a high level of security to the IoT ecosystem and management
  - The Hub should be easy to update
  - The Hub should be able to monitor, audit, and report its update and patch status
  - The Hub may be able to auto-update if allowed

- ハブは、レポート能力備えた、アップデート／パッチのログを保持する必要がある。以下の例を参照：
  - ハブは、タイムスタンプやスケジュールされたアップデートなどの、過去／将来の更新に関する情報をログに記録する必要がある。
  - ハブは、アップデートの履歴／検証に関する情報を、ログに記録する必要がある。
  - ハブは、自動／手動での入力をサポートする必要がある。
- ハブは、アップデート／パッチの適用を、可能な範囲で一元的に管理する必要がある。以下の例を参照：
  - ハブは、IoTデバイスのアップデートをキャッシュする場合がある。
  - ハブは、接続が制限的／断続的なデバイスのアップデートも行い、また、マルチパートのアップデートにも対応する必要がある。
  - ハブは、更新の自動／手動で開始されるアップデートをサポートする必要がある。
  - ハブは、さまざまなソースに基づくアップデートを、管理する必要がある（例：エンタープライズやメーカーがプッシュするもの）。
- ハブは、IoTのエコシステム／マネージメントに対してハイ。レベルのセキュリティを提供するために、自身を可能な限り最新の状態に保つ必要がある。
  - ハブは、容易にアップデートできる必要がある。
  - ハブは、自身のアップデート／パッチのステータスを監視／監査／報告できる必要がある。
  - ハブは、許可されている場合において、自動的にアップデートしても良い。

3.4.3 Manage Device Identity and Authorization

Device identity is not a primary focus of this proposed Hub architecture. However, it is worth noting that identity has a useful role in supporting security functions enabled by this Hub architecture – such as authentication, roots of trust, and device lifecycle management. For instance, identifying a device can support assigning or revoking device privileges and make tracking and implementing updates easier.

デバイスIDは、ここで提案されるハブ・アーキテクチャにとって、主たる論点ではない。ただし、IDには、このハブ・アーキテクチャが実現する、認証／信頼のルート／デバイスのライフサイクル管理などのセキュリティ機能を、サポートする上での有用な役割があることに注意してほしい。たとえば、デバイスが識別されると、デバイス特権の割当／取消がサポートされ、アップデートの追跡／実装が容易になる。

The specific technologies, services, or other resources that may be used to assign and/or manage device identity is not within the scope of this proposed Hub architecture. No identity solution or management tool is presumed or prescribed here. There are a range of solutions, both available and developing, that can be successfully used in IoT deployment.

デバイスIDの割当／管理に用いる特定のテクノロジー／サービス／リソースなどは、ここで提案されるハブ・アーキテクチャの範囲外になる。つまり、ここではIDソリューションや、そのための管理ツールは、想定／規定されていない。ただし。ここで提供されるソリューションは、利用可能なものと開発中のものがあり、どちらもIoTデプロイメントにおいて適切に使用できる。

In addition, there may be situations when sharing or assigning a device identity may not be desired by either party. For instance, personal devices brought onto the Enterprise network by employees, such as smart watches or fitness trackers. Personally identifiable information, particularly that which is not required for business functions, is not in scope of this paper and should be handled in a manner consistent with local data protection and privacy policies.

さらに、デバイスIDの共有／割当が、いずれのグループでも好まれない場合もある。たとえば、スマート・ウォッチやフィットネス・トラッカーなどの、従業員がエンタープライズ・ネットワークに持ち込んだ個人用デバイスが挙げられる。個人を特定できる情報であり、とりわけビジネス環境で必要とされない情報は、このペーパーの範囲外であり、ローカルデータ保護やプライバシーに関するポリシーと、一致する方法で処理される必要がある。

Taking this into consideration, in an IoT ecosystem, it should be possible to assign identity to all devices or groups of devices as appropriate. Identity may be provided via a variety of resources including, but not restricted to:

これらの点を考慮すべきであるが、IoTエコシステムでは必要に応じて、すべてのデバイスまたはデバイス・グループに対して、IDを割り当てることができるはずだ。IDは、以下を含むが多様なリソースを介して提供されるだろうが、これらに限定されるわけではない：

- Manufacturers
- Private and bespoke identity schemes
- Third party solutions or services
- Hub solutions

- マニュファクチュア
- プライベート／オーダーメイドIDスキーム
- サードパーティ・ソリューション／サービス
- ハブ・ソリューション

If an Enterprise decides to implement an identity scheme, a Hub may:

エンタープライズが、なんらかのIDスキームを実装すると決定した場合、ハブは以下のことを行うだろう。

- Improve overall IoT ecosystem management and security
- Provide a centralized database for device and/or identity management
- Provide flexibility to assign a device to one or multiple groups
- Provide flexibility to assign attributes and authorizations to a device and/or group of devices

- IoTエコシステム全体の管理とセキュリティを向上させる
- デバイス／IDを管理するための一元化されたデータベースを提供する
- デバイスを単一／複数のグループに割り当てる柔軟性を提供する
- デバイス／デバイス・グループに対して属性と承認を割当てる柔軟性を提供する

3.4.4 Managing Device End-of-Life

An IoT device's lifetime can be unique to each deployment. For an IoT device, the end of life will most likely be the result of a number of factors, including but not limited to:

IoTデバイスのライフタイムはは、それぞれのデプロイメントごとに固有のものとなるだろう。IoTデバイスの場合、ライフタイムの終わりは、以下のような多様な要因の結果になるだろうが、それらに限定されるわけではない:

- Manufacturer end-of-sale or support (such as discontinuing updates and patches)
- Enterprise upgrade or solution change including integrating new devices and decommissioning old devices
- Change of ownership, where an Enterprise may inherit or transfer ownership of IoT systems (for example in the case of office location change)

- メーカーにおける販売／サポートの終了（アップデート／パッチの中止など）
- エンタープライズにおけるアップグレードまたはソリューションの変更。新しいデバイスとの統合や、古いデバイスの廃止などが含まれる。
- 所有権の変更。エンタープライズが、IoTシステムの所有権を継承／譲渡する場合がある（たとえば、オフィスを引っ越す場合）。

Security practices included in this architecture support good practices for end-of-life management. For instance, there are a number of security practices that need to be considered when managing end-of-life, including but not limited to:

このアーキテクチャに含まれるセキュリティ・プラクティスは、保守の終了管理に関する適切なプラクティスをサポートする。たとえば、サポート終了を管理する際に考慮すべきセキュリティ・プラクティスには、以下のようなものがあるが、それらに限定されるわけではない：

- Managing permissions and revoking authorization
- Understanding what Enterprise information is accessible by the device and removing or protecting this data
- Data erasure – permanent deletion of any settings, user account information etc.
- Decommissioning or transferring device identity
- Precautions for transferring device ownership, such as data erasure, factory re-set, etc.

- 権限の管理と承認の取り消し。
- 対象となるデバイスからアクセス可能なエンタープライズ情報を理解し、それらのデータを削除／保護する。
- データの消去。設定情報やユーザー・アカウント情報などの完全な削除。
- デバイスIDの廃止または転送。
- データの消去や、ファクトリー・リセットなどの、デバイスの所有権を譲渡する際の心得。

A Hub architecture provides a central location to query information about the device, its authenticity, authorizations, network access and in some cases execute the necessary actions to revoke permissions and decommission a device and/or the Hub itself from the IoT ecosystem.

ハブ・アーキテクチャは、デバイスおよび、その真正、承認、ネットワーク・アクセスなどに関する情報を、クエリーするためのセンタライズされた場所を提供する。また、場合によっては、IoTエコシステムにおけるアクセス許可の取り消しや、デバイスやハブ自体を廃止するために必要なアクションを実行する。

3.4.5 Examples of Lifecycle Management Tools

While this architecture does not prescribe any one specific solution or make assumptions regarding the IoT security requirements of the Enterprise, below are examples of how a Hub architecture may interface with or support lifecycle management IoT ecosystem:

このアーキテクチャは、特定のソリューションを規定するものでもなく、エンタープライズIoTのセキュリティ要件にについて仮定するものでもない。したがって、以下の項目は、ライフサイクル管理IoTエコシステムに対して、ハブ・アーキテクチャがインターフェースを持ち、また、サポートする方式を示す例となる。

- A Hub should monitor the traffic in and out of the IoT network. For instance, there might be coffee machines communicating with the office manager as well as sending usage statistics to the supplier once a day. However, if outward coffee machine traffic suddenly spikes to once a minute then the Hub may alert the IoT manager to suspicious activity. It may be that the device has been compromised, such as infected by malware utilized in a DDoS attack. In this case, the IoT manager can immediately take the device offline

- Some updates may need to be pushed to devices by IoT managers. For instance, a Hub can receive alerts from a smart board manufacturer when an update or patch is available. The IoT manager can then immediately push the update to the device or place it in a queue for updating outside of normal business hours. Once the update has been installed, the Hub can receive notification and update the patch log for the smart board

- A Hub will have a user-friendly interface to manage IoT devices. An Enterprise adopting solutions from multiple vendors – such as light bulbs form Vendors A and B and door locks from Vendor C – may find a variety of identifiers, not necessarily user friendly, attached to the devices (such as lb_12345 or lock_jfk). In the Hub interface, the IoT manager can assign unique identifiers and location or vendor attributes to devices (such as “Light: vendor A, Office 245” or “Door Lock: Vendor B, meeting room A”). The IoT manager can then search by vendors, locations, or type of IoT solution to oversee, grant or revoke authorization, and delete data relating to a device or group of devices

- ハブは、IoTネットワークに出入りするトラフィックを監視する必要がある。たとえば、コーヒー・マシンの場合、オフィス・マネージャーと通信すれば、使用統計を毎日サプライヤーに送信することもある。ただし、コーヒー・マシンから外部へ向かうトラフィックが、突然1分に1回に急増した場合、ハブはIoTマネージャーに対して疑わしいアクティビティを警告するだろう。マルウェアに感染してDDoS攻撃されるなどの、デバイス侵害が生じた可能性がある。この場合、IoTマネージャーは直ちに、デバイスをオフラインにできる。

- 一部のアップデートでは、IoTマネージャーからデバイスにプッシュする必要性が生じるだろう。たとえば、あるハブは、スマートボードのアップデート／パッチが利用可能になったときに、その製造元からアラートを受信できる。そのIoTマネージャーは、すぐにアップデートをデバイスにプッシュするか、営業時間外にアップデートするためにキューに入れることができる。アップデートがインストールされると、ハブはノーティフィケーションを受信し、スマートボードのパッチ・ログを更新する。

- あるハブは、IoTデバイスを管理するための、ユーザーフレンドリーなインターフェースを持つだろう。複数ベンダーのソリューションを採用している企業は（ベンダーAとBの電球や、ベンダーCのドアロックなど）、デバイスに接続されている、ユーザーフレンドリーとは無縁な、多様な識別子を見つける可能性がある（lb_12345 や lock_jfk など）。対象となるハブ・インターフェイスにおいて、IoTマネージャーは固有の識別子／ロケーション／ベンダー属性をデバイスに割り当てることができる（Light: vendor A, Office 245 や Door Lock: Vendor B, meeting room A など）。続いて、IoTマネージャーは、ベンダー／ロケーション／IoTソリューションの種類などで検索し、承認の付与／取消を確認した後に、デバイス／デバイス・グループに関連するデータを削除できる。

3.5 Hub Device Security

In the end, the Hub architecture presented here is based on a central device and user interface as the foundational element of the Enterprise IoT ecosystem and security. Hub device security and development are not the focus of this document, but it is worth noting that the device must include robust security. This includes features such as:

結局のところ、ここで紹介するハブ・アーキテクチャは、エンタープライズIoTのエコシステムとセキュリティの基本要素である、センタライズされたデバイスとユーザー・インターフェイスをベースにしている。ハブ・デバイスのセキュリティとデプロイメントは、このドキュメントの論点ではないが、このデバイスが堅牢なセキュリティを必要とする点に注意してほしい。 具体的には、以下の機能が含まれる：

- User access permissions that support best practices in system and information security
- Ability to securely store sensitive information such as roots of trust
- Alerts and notification of anomalies
- Security considerations for web and mobile user interfaces as well as network connections
- Secure Boot

- システムおよび情報のセキュリティにおいて、ベスト・プラクティスをサポートするユーザー・アクセス許可
- 信頼のルーツなどの、機密情報を安全に保存する能力
- 異常に関するアラートとノーティフィケーション
- Web／Mobileユーザー・インターフェイスとネットワーク接続に関するセキュリティの考慮
- 安全なブート

The Hub device should adopt security best practices. There are public resources available that help Enterprises as well as developers implement security best practices into their IoT solutions. One example is the IoTSF's "IoT Security Compliance Framework" [ref 1]. In this document, security compliance frameworks are laid out for a range of topics related to the four main Hub functions and support capabilities included in this Hub architecture. The compliance framework sections as presented here are relevant to Hub device security and development and are mapped to the Hub-based reference architecture below.

このハブ・デバイスは、セキュリティのベスト・プラクティスを採用する必要がある。IoTソリューションに対して、セキュリティのベストプラクティスを実装する企業と開発者は、有用なオープン・リソースを利用できる。ひとつの例は、IoTSF の IoT Security Compliance Framework [ref 1] である。このドキュメントでは、セキュリティ・コンプライアンスのフレームワークが説明されている。具体的には、このハブ・アーキテクチャに含まれる、4つの主要なハブ機能とサポート機能に関連する、さまざまなトピックとなる。ここに示されている、コンプライアンス・フレームワークのセクションは、ハブ・デバイスのセキュリティとデプロイメントに関連しており、以下のハブ・ベース・リファレンス・アーキテクチャにマッピングされている。

Hub Functions	Compliance Framework Sections
Network Management	• Cloud and network elements • Secure supply chain and production
Connecting Devices Securely	• Device wired and wireless interfaces • Authentication and authorization • Encryption and key management for hardware • Configuration
Lifecycle Management	• Device hardware and physical security • Device software • Device operating system • Device ownership transfer
Information Security	• Business security processes and responsibility • Web user interface • Mobile application • Privacy

Table 3 IoTSF Compliance Framework Mapping

4 References and Abbreviations

4.1 References

The following references are used in this document:

1. IoTSF "IoT Security Compliance Framework": https://www.iotsecurityfoundation.org/best-practice-guidelines/

2. IETF "Key words for use in RFC's to Indicate Requirement Levels" : https://www.ietf.org/rfc/rfc2119.txt

3. NIST Computer Security Resource Center "Roots of Trust": https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust

4. NIST SP 800-57 Part 1 Rev. 4 "Recommendation for Key Management, Part 1: General" https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final

5. NIST SP800-57 Part 3 Revision 1" NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application - Specific Key Management Guidance" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

6. FIPS PUB 140-2, Security Requirements for Cryptographic Modules https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

7. UK Government DCMS "Secure by Design report": https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

8. IoTSF "Application Note: Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT": https://www.iotsecurityfoundation.org/wp-content/uploads/2018/03/RELEASE-DCMS_Principles_Application_Note_07_03_2018.pdf

9. ISO/IEC "Information Technology – Security techniques – Information security management systems – Overview and vocabulary: https://standards.iso.org/ittf/PubliclyAvailableStandards/

10. IoTSF "Make it safe to connect: Establishing principles for Internet of Things Security": https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

11. IoTSF "Secure Design - Best Practice Guidelines L Software Update Policy": https://www.iotsecurityfoundation.org/best-practice-guidelines/

12. NCSC UK "Guidance - Provisioning and securing security certificates" https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates

13. European Commission "2018 Reform of Data Protection Rules": https://ec.europa.eu/info/

14. European Commission "Latest NIS Cooperation Group's guidelines for implementing the NIS Directive https://ec.europa.eu/digital-single-market/en/news/nis-cooperation-groups-guidelines-implementing-nis-directive-and-addressing-wider-cybersecurity

15. Office of the Federal Register (US). "CISA 2015 Final Guidance Documents": https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

16. NIST Computer Security Resource Center "Guidelines on Hardware - Rooted Security in Mobile Devices (Draft)": https://csrc.nist.gov/publications/detail/sp/800-164/draft

17. IETF Bootstrapping Remote Secure Key Infrastructures (BRSKI) draft 16, June 21st 2018: https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-16

4.2 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply:

PKI	Public Key Infrastructure
TRNG	True Random Number Generator
TBC	To Be Confirmed
TBD	To Be Determined
TLS	Transport Layer Security

5 Appendix A – Sample Threat Modelling

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Employing spoofing of IP addresses and/or user datagram protocol (UDP) to obtain credentials to gain unauthorized access to a device Address resolution protocol (ARP) spoofing used to redirect data traffic to the attacker Spoofing notifications or alerts Sending spoofed packets to influence the functioning of a device (e.g. stop, start, or modify data collection and transfer) Enterprise user unknowingly being directed to a spoofed website of a cloud service provider	Update and patch devices to prevent vulnerability exploitation Roots of trust to support trusted identity and access Manage device identity to support a compromised devices' authorization and access privileges and end of life provisioning Implementing gateways and firewalls to identify suspicious traffic	Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Roots of Trust [3.3.3] Update and Patch [3.4.2] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Tampering	Tampering with a connected door lock to gain unauthorized control Covertly modifying a sensor's data sharing permissions Tampering with software to modify permissions, install spyware or backdoors Tampering with data, impacting the trust, and possibly business processes, in the IoT ecosystem	Use roots of trust to support non-repudiation Secure boot and update to ensure software and hardware are modified by trusted sources Secure management of access controls Monitor and audit device status and traffic flow to identify unauthorized activities Set up new devices or services in a staging system to prevent tampered devices from accessing the live network	Separation of Systems [3.2.2] Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1] Secure Boot [3.3.2] Roots of Trust [3.3.3]

Repudiation	Sensor data is modified in transit to the cloud service and Enterprise metrics are affected Device A receives a command seemingly from Device B but it was sent actually by an unknown source and leads to malfunction A staff group share a group password/authentication process for accessing a system	Use of digital certificates to support secure identity of users and devices Public key infrastructure to manage and revoke digital certificates and roots of trust Secure boot and update to ensure only authorized modification of software and hardware Information security best practices – managing individual user access controls	Authentication and Authorization [3.3.1] Roots of Trust [3.3.3] Secure Boot [3.3.2] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Information Disclosure (Data Breach)	Corporate espionage and black hat hacking Disgruntled employee accesses and copies confidential or sensitive information Diagnostics information shared with an OEM which discloses proprietary Enterprise information Unauthorized access to security cameras Password leaks or unauthorized password/credential modification Packet capture via man-in-the-	Monitor and audit traffic on and outside of the local IoT network Alerts for suspicious data traffic Privilege-based or other fine-grain user authorization management Adoption of information security management best practices Separating business and IoT networks Encryption of data	Local IoT Network [3.2.1] Gateway and Firewalls [3.2.3] Authentication and Authorization [3.3.1] Monitoring and Audit [3.4.1] Device Identity and Authorization [3.4.3] Managing End-Of-Life [3.4.4]
Denial of Service	Using exploits in connected devices to execute a DoS attack on the Enterprise website Using exploits in connected devices to disrupt normal business functions of the Enterprise's connected systems Using exploits in connected devices to execute a DoS or	Traffic monitoring and management (ingoing and outgoing) Use of gateways and firewalls to monitor and block traffic Blocking devices from communicating outside the LAN or Enterprise Restricting access to	Local IoT Network [3.2.1] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1] Update and Patch [3.4.2]

	DDoS attack on a third-party network or site Using exploits in connected devices to execute a DoS or DDoS attack on another IoT device in the network	command/control functions of devices Taking compromised and irreparable devices out of the Enterprise IoT ecosystem securely	Authorization [3.4.3] Manage End-Of-Life [3.4.4]
Elevation of Privilege	A smart device zero-day exploit that allows a third party onto the LAN Unauthorized access of a cloud service provider's system enabling access to the Enterprise business network Gaining high-level privileges which enable command and control of a thing-bot	Lifecycle management and decommissioning old or compromised devices Separation of IoT and business networks to discourage privileged users from accessing non-relevant business information Privilege-based or other fine-grain user authorization management to prevent access to non-relevant information, controls and	Local IoT Network [3.2.1] Authentication & Authorization [3.3.1] Monitor and Audit [3.4.1] Device Identity and Authorization [3.4.3] Managing End-Of-Life
Regulatory Non-Compliance	Inability to or difficulty in proving compliance for audit purposes Lack of easily applied metrics to measure compliance or identify security shortfalls Need to prove compliance after a data breach to show due diligence	Log and report on security features and ecosystem management Enable security best practices Identify, manage, and update regulation compliance measures	Highly dependent on regulatory requirements. Common examples are: Gateways and Firewalls [3.2.3] Authentication & Authorization [3.3.1]
Unsupported endpoint management	Out of date devices with known exploits or bugs being exploited to access IoT networks Devices with outdated software or firmware Inability to encrypt data or assign a root of trust Inability to remotely manage end-of-life	Monitor data traffic and enable alerts for suspicious traffic Manage authorization and access to devices Physically manage updates or push updates where possible Create a secure environment for devices – separate devices from WAN and	Local IoT Network [3.2.1] Separation of Systems [3.2.2] Gateways and Firewalls [3.2.3] Monitor and Audit [3.4.1] Update and Patch

		business networks Set up devices with minimal security features in a testing or staging system to prevent impact on local IoT network	Manage End-Of-Life [3.4.4]

6 Appendix B – Note on Information Security Best Practices

It is assumed that information security best practices will be implemented with IoT deployments, be structured in a way that best meets the needs of the Enterprise, and is in compliance with relevant regulations such as local data protection and privacy regulations. Information security best practice are not the focus of the architecture, but more information on how they relate can be found in Appendix B.

Because many IoT solutions are wholly or in part provided via a cloud-based service it is important to note that an Enterprise should assess risks associated with data transfers outside the organization. This may include business operational data (such as client information), sensor data (such as lights and temperature), or other types of data which provide information about the Enterprise. Data which is sensitive or business-critical may require additional levels of security which is best managed within the organization, while others may find service providers better-suited to some types of information management and security. Risks associated with external and/or internal data management will be unique to the Enterprise, therefore no assumptions are made here about the Enterprise's chosen solution.

Information security best practices should be incorporated throughout the IoT system were necessary, for example:

- Data security at rest and in transit
- User authentication and access privileges
- Securing sensitive information (e.g. keys and certificate management)

For these reasons there is not a dedicated information security section of this Hub architecture. However, relevant information on this topic is provided where needed.

For more information on this topic specifically, Enterprises can consult a range of resources regarding information security standards and best practices made publicly available through independent organizations, standards bodies, and national governments including IoT Security Foundation, ISO, BSI, NIST, and NCSC.

www.iotsecurityfoundation.org