IoT における ID/アクセス管理 要点ガイダンス

IoT Working Group

Presented by CSA cloud security alliance®

日本語バージョン 1.0

日本語版の提供について

本書「**IoTにおけるID/アクセス管理　要点ガイダンス**」は、CSAが公開している「**Identity and Access Management for the Internet of Things – Summary Guidance**」の日本語訳です。本書は、原文をそのまま翻訳したものです。また、本書内で参照されているURL等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。また、この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。
本書は、一般社団法人日本クラウドセキュリティアライアンス　IoT ワーキンググループの以下のメンバーにより作成されました(順不同、敬称略)。

変更履歴

日付	バージョン	変更内容
2016 年 4 月 4 日	日本語バージョン 1.0	

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

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

2016 年 4 月 4 日

謝辞

イニシアチブメンバー

Arlene Mordeno, Edgile
Brian Russell, Leidos

執筆者

K S Abhiraj
Amit Pick
Srinivas Tatipamula
Aaron Guzman
Tom Donahoe
Vinay Bansal
Jay Douglas
Sabri Khemissa
Raghavender D
Mike Flegel
Abhik Chaudhuri
Drew Van Duren
Sudharma Thikkavarapu
Shyam Sundaram
Ayoub FIGUIGUI, CGI Business Consulting

CSA オフィシャルメンバー

John Yeoh
JR Santos

リーダーからのメッセージ

> “Internet of Things (IoT)は、消費者向けおよびビジネス向けの環境において、急成長を遂げている。”

Internet of Things(IoT)は消費者向けおよびビジネス向けの環境において、急成長を遂げている。CSA は、IoT のソリューションを実装しようとしている関係者に対して、信頼できるガイダンスを提供すべく、IoT ワーキンググループを立ち上げた。この文書は、IoT ソリューションをセキュアに実装し、導入する使命を帯びた IT スタッフに対して、容易に理解できる推奨事項を提供するための一連の要点ガイダンスの最初のものである。この文書では IoT におけるアイデンティティおよびアクセス管理（IAM）についての考察を行っている。

CSA IoT WG が 2015 年 4 月に出した「IoT 早期導入者のためのセキュリティガイダンス」と題するレポートの中でもこのテーマ（IAM）は議論されている。しかしながら、現実にこの技術分野は常に変化している。このガイダンスで、CSA IoT WG は、組織内で IoT プログラムのための IAM を確立するために、関係者が取り組みやすい形の推奨事項集を提供しようと試みた。

実際、こうした IoT におけるアイデンティティ管理のリサーチと標準化に向けて取り組んでいる他の団体もあることから、我々はこの文書でも、可能な部分ではそれらを参照している。将来的に、我々は CSA 自身のリサーチに加え、これらの団体のリサーチやガイダンスの成果も反映させていくつもりである。

我々は、この文書やその他の IoT ガイダンス文書の作成に尽力してくれた世界中の多くの協力者に感謝したい。とりわけ、この最初の要点ガイダンス文書作成をボランティアとして主導してくれた Arlene Mordeno、 および、この文書の作成に対して有益で実のあるインプットを行ってくれたピア・レビュアーの方々に謝辞を述べたい。

Brian Russell
IoTワーキンググループ　リーダー

はじめに

IoT では、既存の IAM システムが取り扱わなければならないアイデンティティの数に比べて桁違いに多くのアイデンティティを取り扱う必要が生じる。セキュリティ業界は、IAM がもはや（システムの利用者たる）人々の管理を考えていればいいだけではなく、何十万もの、おそらくネットワークに接続された「モノ」の管理をも考えなければならないというパラダイムシフトに直面している。多くの場合、これらの「モノ」は、断続的にネットワークに接続され、おそらくは他の「モノ」やモバイルデバイス、背後にある基盤（システム）などと通信することを求められる。すでに一部では、こうした新しいアイデンティティのエコシステムを Identity of Things (IDoT)と呼び始めている。IDoT では、デバイスと人、デバイスとデバイス、デバイスとアプリケーションやサービスまたは人とアプリケーションやサービスとの関係を取り扱うことになる。

業界は、まだ IoT のデザインと導入に向けて動き出したばかりである。

故に、IoT で繋がった企業において必要な他のセキュリティサービスと IoT の IAM との関係を考えるには最も良い時期だと言える。これには、たとえば資産や暗号鍵の管理に関するサービスなども含まれる。いくつかの事例では、IoT ソリューションベンダは、IoT 資産を相互に接続するための製品の一部として IAM を統合しようとしている。

また、カンターラ・イニシアティブ (https://kantarainitiative.org)が主導して、アイデンティティ・リレーションシップ・マネジメント（IRM）に向けた動きも始まっている。カンターラ・イニシアティブは、既に IRM の柱となる考え方を定義しているが、それらの一部は、（従来の）従業員を対象としたものから、消費者と「モノ」を対象としたものへ、また、企業規模からインターネット規模へ、そして、「境界」を作るよりも、ボーダレスな考え方への変化を促すものである[1]。これらの柱は IoT IAM に必要とされる事項に非常によくあてはまっている。（IoT を導入しようとする）組織は、我々の（セキュリティ）業界が提唱する新しい IRM の考え方について、継続的に情報を得ておくべきである。

IoT のアイデンティティとアクセスマネジメントにおける課題は他にもある。 そうした課題には、どのような多要素認証が必要とされるかについての再考が必要になることや、 組織におけるネットワークに接続された資産のネーミングルールを決める必要があること、などが含まれる。 EU 委員会の IoT 専門家グループによる IoT アイデンティティに関するレポートによれば、「グローバルなスキームで衝突のないユニークなアドレスを割り当てるという課題については、(1)突然ネットワークに現れたり消えたりし、(2) ローカルなもしくはプライベートな（またはその両方の）異なるネットワーク間を行き来し、かつ、(3)そのデバイスの利用者を一意に特定し、もしくは必要に応じてプライバシーを保護するために利用者のアイデンティティを隠蔽できる柔軟性を有する、非常に動的なデバイスをサポートするインフラを用意することが要求される。スマートセンサ、ネットワーク化されたパーキングメーター、自動車もしくはネットワーク化されたヘルスケアデバイスなどのいずれを管理する場合においても、それぞれのデバイスは大規模なシステム内でアドレス可能でなければならず、また、デバイスの名前は、それを証明するための要素（Credential）と紐付いているべきである。」と述べている。

多要素認証に関しては、これまで使われてきた多要素認証方式を、デバイスの認証強化のために、常に利用できるとは限らない。カンターラ・イニシアティブなどによって、コンテキストベースの認証を（多要素）認証プロセスにおける新たな（認証）要素として使用するような研究の必要性が指摘されている。FIDO（USB ベースのハードウエア多要素認証）や CryptoPhoto（スマートフォン通信による多要素認証）など次世代の認証を推進する団体は、組み込み型の相互認証による強固な認証方式を提案しており、そのいずれもが、たとえそれがキーボードや画面を持たないものであっても、IoT デバイスの認証に適した方式である。

我々は今、IoT IAM を意識する新たな段階に入ったのだから、

この分野における標準化の作業と動きを合わせておくことも、また重要である。たとえば IETF は、「制約のある環境における認証、認可」（ACE: Authentication and Authorization for Constrained Environments: http://datatracker.ietf.org/wg/ace/documents/) の傘下で、一連の作業を行っている。IETF の ACE ワーキンググループは、既存の IoT プロトコルへの改良作業を行っている。たとえば、Delegated CoAP プロトコル（リソースが限られたデバイスが、Authorization Manager と呼ばれるリソース制約が少ないデバイスに認証や認可に関する作業を委任するに際しての仕様）は、制約の大きいデバイスに対するセキュリティソリューションによるハードウエア負荷を軽減しようとしているのである。

[1] https://kantarainitiative.org/irmpillars/ 参照

IoT の ID/アクセス管理に関する要点ガイダンス

01

組織に存在する IAM や GRC のガバナンスフレームワークへの統合の下に、IoT を実装すること。次のステップを含めて検討すること。

a. IoT デバイスの共通名前空間を定義する。

b. 組織にあるモノ(things)に適用でき、デバイスと必要な識別子の有効期限に対応してカスタマイズすることができる、拡張可能な ID ライフサイクルを確立する。

c. ID ライフサイクルの中で、IoT デバイスの明確な登録プロセスを確立する。特定の IoT デバイスが扱うデータの機微の程度に応じて、登録プロセスの厳格さを設定すべきである。

d. センサーや他の IoT コンポーネントからの特定のデータフローに対して、セキュリティ保護（機密性、認証、認可）の適用レベルを設定する。

e. IoT デバイスに対するローカルアクセス（例えば管理用ローカルアクセス）の明確な認証・認可手続きを定める。

f. データ分類ごとに求められるプライバシー保護を定義する。そのためには、個人識別情報(PII)のプライバシー保護を実現するフレームワークの参照定義を作成することが有効である。

g. 外部の組織に特定の種類のデータにアクセス権を与えるかどうかを決定し文書化する。

h. ネットワークとたまにしか接続しない IoT デバイスの認証・認可をどのように実行するかを定義する。

i. 組織のアクセス制御方針に従い、IoT に適用する ID アクセス制御要件を明確にする。

各ビジネスユニットのリーダーは、上記の全てを理解する必要がある。

02

管理アクセス用デフォルトパスワードを変更せずに IoT リソースを配備しないこと。もし可能であれば、ローカルアクセス機能しか持たない IoT デバイスは配備しない。むしろ、全ての IoT リソースを企業の IAM システムに統合するよう試みること。このガイダンスは企業ネットワークに接続する個人向けの IoT デバイスにはあてはまらないことに注意する。この分野の IoT デバイスには、BYOD のデバイス登録に要求されるものに類似した新たな考え方を適用することが必要であろう。

03

従来型の IAM からアイデンティティ・リレーションシップ・マネージメント（IRM）への移行を評価すること。IRM は従来型の IAM よりも

IoT に適しており、従業員を対象としたものから「消費者」と「モノ」を対象としたものへ、また、企業規模からインターネット規模へ、そして、「境界」に閉じたものよりもボーダレス、というような考え方の組み合わせを基礎にしている。組織が必要とする IoT の ID にフィットする可能性のある IRM ベンダーによるソリューションを探して評価すること。

04

システムレベルの脅威モデルに基づき認証・認可スキームを設計すること。個々の製造元の IoT 実装を評価し、適用対象の標準または対象となるガイダンスを厳守するベンダーを選択するか、BuildItSecure.ly や OWASP のような業界セキュリティグループのベストプラクティスに従うベンダーを選択すること。システムの脆弱性を考慮すること。

05

IoT 認証のためのスマートフォン。モバイルデバイスと通信ネットワークは IoT にとって大きな役割を果たす。スマートフォンは我々の周りにあるモノ(things)にアクセスするための認証ステップの１つとして利用される可能性を秘めている。スマートフォンを強力な認証要素としている機能を、他のデバイスに密に結びつける必要がある。次世代スマートフォンは指紋のような従来のバイオメトリクスの他に、フロントカメラを使った顔認識、音声認識、ジェスチャーや手振りの認識のような異なるタイプの認証メカニズムを利用する道を開く。これらのスマートフォンを、IoT デバイスの企業に閉じたローカル認証に利用できるだろう。

06

最初に ITU-T Y.2060 を使用した IoT 実装の参照アーキテクチャーを作ること。IoT 参照アーキテクチャーはインフラ内にある全ての IoT デバイスにまたがる認証、認可、アカウンティング(AAA)の一貫した実装を可能とし、テクノロジースタックの様々なレイヤーにおける個々の機械から機械ネットワークまでのあらゆるレベルのシステムによる全てのアクセスをテストするために利用することができる。組織内の最も脆弱なデバイスを識別し、可能な限り多要素認証を適用すること。

07

IPv6 の導入を計画すること。産業界はまだ長い移行期間にあるため、組織は完全には IPv6 には移行していない。IPv4 で使うためにデザインされた多くの IoT デバイスがあるため、M2M 実装シナリオにおいて、IPv4 で使うためにデザインされたデバイスを、IPv6 で使うためにデザインされた IoT デバイスと、どうやって通信できるようにするかという課題に関する計画を、今のうちに立てることが必要である。これを実現するために、これらのデバイスと他の必要なサービスが通信できるように SDN（Software Defined Network）メカニズムを検討すること。

08

組織内の IoT デバイスに対する証明書の発行をサポートするために PKI 環境の設計の更新を検討すること。デバイス認証のため、TLS(Transport Layer Security)または他のプロトコルネゴシエーション時に機密性を保つため、ならびに他のアクセス制御メカニズムを統合する際に様々な他の ID バインディングをサポートするために、可能な限り証明書を使うこと。PKI アーキテクチャーが、失効確認、信頼管理、エンロールメント/登録手続き、そして侵害からの回復のような標準サービスをサポートするようにすること。より小さな IEEE 1609.2 クレデンシャルフォーマットのような IoT に最適化された代替証明書タイプを評価すること。進化した IoT エコシステムをサポートする手段である OCSP（Online Certificate Status Protocol）ステープリングあるいは DANE(DNS ベースの認証)のような追加サービスを評価すること。これらの技術はセキュリティを改善し、OCSP サーバとの通信を必要としないため、ネットワークやセンサーの負荷を減らすことができる。自組織の PKI が大量のデバイスに証明書を発行できるように拡張性を持つことを確かめること。

09

デバイス製造元に IoT 関連データを共有する計画を策定すること。デバイスの製造元はデバイスの状態をモニターしたり、統計情報を記録したり、顧客にサポートを提供できるようにするためにデバイスデータにアクセスし続けようとする。このデータは収集され、様々なタイプのデータベースに保管される。これらのバックエンドにあるデータストアのための認可モデルを実装し、1)関連したプライバシー規則に準拠し、2)製造元や他のサードパーティーが必要とする最小限のアクセスを可能にするようにする。

10

消費者が、（事業者に）アクセスさせるべきプロファイルデータを指定したり、消費者のプロファイルデータへのサービスからのアクセスに対する同意を与えたりする機能を持つ AAA サーバを実装すること。IoT 実装はそのようなサービスの１つである。これは、消費者や患者のような外部の主体に関する管理が必要である。それによって、消費者や患者は自分のプロファイル情報のどの属性について誰と共有することを認めるかを選択することが可能になる。多くの場合、このためには、AAA サービスを、データの取り扱いに関する消費者やビジネスパートナーの選択を管理するサードバーティーサービスと、結びつける必要がある。

11

ID 管理システムを建物の物理アクセス管理システム（または入退管理システム）と統合することを検討すること。これにより、ID カードでアクセスできるドアやエントランスを選択的に割り当てるような更なるセキュリティ対策を可能にする。これらのセキュリティ強化は IoT デバイスに対する物理的保護を改善するだろう。

12 **ID 管理ワークフローにより厳しい（認可）ロジックを実装すること。**これにより、ある人がアクセスガバナンスフレームワークによって定められた必要な資格要件を満たしていないのであれば、IoT 関連システムやデバイスへのアクセスを予防的に制限するようにできる。資格要件の例として、トレーニングの受講や身元調査などが挙げられる。

13 **管理者がシステムやデバイスにアクセスしたり監視できるように特権ユーザー管理システムを実装すること。**これには、特権セッションのモニタリング、サービスアカウントのパスワード保護、頻繁なパスワード変更が含まれる。

14 **可能な限り、現状の資産管理を IoT デバイスの棚卸しと台帳作成ができるように拡張する。** IoT デバイスをリスクに基づいて分類し管理者を割り当てる。アクセス記録（の仕組み）を変更し、資産管理者、資産の所在、必要な廃棄もしくは資産ライフサイクルのワークフローを記録できるようにする。資産ライフサイクル管理の自動化と監査を行うサービスデスクシステムを導入し、物理資産の廃棄が記録システムにも反映されるようにする。

15 **障害や事故が起きた時の対応を詳細に記述した計画作成に取り組むこと。**例：インシデント対応計画（Incident Handling or Incident Response plan）。この計画はインシデント管理プロセスおよびワークフローに組み込まれるべきである。

16 **人とデバイスを関連付けるマッピングを作成すること。**特定のデータセットに対して人に許可された行為について明示的な許可を示すことを含む。ユーザーとモノの両面からアクセス管理を適用する。IoT データへのユーザーアクセスに対しては、可能な限り多要素認証を実装すること。

17 **センサーノードには、その位置付けとサービスのためのセキュリティ要件に基づいて、有効な AAA 機構を開発すること。**無線センサーノードは IoT 実装の主要要素だが、無線網の中でセンサーノードの AAA は、電力と計算能力の制約からフールプルーフが実現できていない。特定のセンサーノードによってもたらされるリスクに基づいて必要な認証の強度を決める補助手段として（センサーノードの）位置付けを検討する。位置付けの例として設置場所/座標、時刻、アクセスされるエンドデバイス/システム、送受信されるデータタイプなどが挙げられる。

攻撃シナリオでは、センサーに関する情報が容易に盗まれ、改ざんされ、あるいはなりすまされることに注意する

こと。センサーに関する情報が誤って見落とされる危険性と正当なユーザーが誤ってブロックされることによる潜在的な危険性（例：不良なデバイスクロック、アップグレードされたエンドポイント、予期しない場所からの正当なアクセス、GPS 信号の損失など）も心に留めておくこと。センサーノードに対して、最適な AAA メカニズムを決めるために、脅威モデリングを実施すること。

18

標準に基づく IoT プロトコルに組み込まれたセキュリティ制御を活用すること。たとえば、CoAP、 DDS や REST のようなプロトコルを用いて、異なる製造元の IoT デバイス間で相互運用可能な認証および認可トランザクションを可能にする。

次の表では、どのようなタイプの認証が利用可能であるかについて、様々な共通の IoT 通信のプロトコルとアサーションを示している。採用したプロトコルは、可能であれば、上記の推奨に準拠した統合認証アプローチを用いるべきである。

IoT プロトコルおよび認証オプションの例

プロトコル	m2m 認証オプション	分析
MQTT	ユーザ名とパスワード	MQTT はユーザ名とパスワードを伝送できるが、パスワードの長さは 12 文字までに制限される。ユーザ名とパスワードは平文で転送されるため、 MQTT の利用においては、 TLS が必須となる。
CoAP	事前共有鍵 公開鍵 電子証明書	CoAP はデバイス間通信において複数の認証オプションをサポートする。データグラム TLS（ DTLS） と組み合わせることで、より高いセキュリティを確保できる。
XMPP	複数の認証方式（プロトコル）をサポートする	XMPP は SASL(Simple Authentication and Security Layer – RFC4422)を介して、 様々な認証方式をサポートする。 一方向の匿名認証や双方向の暗号化パスワードを使った相互認証、電子証明書、 SASL の抽象化レイヤで実装可能なその他の方法がある。

プロトコル	m2m 認証オプション	分析
DDS	RSA や DSA アルゴリズムを使用した X.509 証明書（ PKI）トークンを使用した認証	Object Management Group による DDS(Data Distribution Standard)のセキュリティ仕様では、エンドポイント認証に加え、その後実施されるメッセージデータの（ HMAC 等を使用した）発信元認証のための鍵交換を提供する。電子証明書や、様々なタイプの ID・認可トークンがサポートされている。
Zigbee	事前共有鍵	Zigbee は、マスター鍵（オプション）またはネットワーク鍵（必須）または、アプリケーション鍵を使ったネットワークレベル認証とアプリケーションレベル認証の両方を提供する。
Bluetooth	共有鍵	Bluetooth は標準ペアリング及び単純ペアリングのという二種類のオプションによる認証サービスを提供する。標準ペアリング方式は自動化されている。単純ペアリングでは、人が介在して（単純な Diffie-Hellman 交換の後で）二つのデバイス間で交換された鍵が同じハッシュを示すことを検証する。Bluetooth では、一方向の認証と相互認証の両方を提供する。 Bluetooth のセキュアで簡単なペアリング方式では、デバイス間認証のために、「とりあえず動く」、「パスキー入力でのペアリング」「出荷時設定で動作する」といった選択肢が可能である
Bluetooth-LE	データ暗号化なし CSRK10 による認証 IRK11 によるデバイスの識別とプライバシー確保	Bluetooth-LE は、 Bluetooth の世界に二要素認証を提供する。 LE セキュアコネクションペアリングモデルでは、デバイスの能力に応じて数種類のアソシエーションモデルを利用できる。また、鍵交換には楕円曲線 Diffie-Helman 方式が使用される。

プロトコル	m2m 認証オプション	分析
HTTP/ REST	ベーシック認証（平文または TLS） OAUTH2	HTTP/REST は、一般に認証と機密性維持のために TLS プロトコルのサポートが必要である。ベーシック認証（識別情報が平文で渡される）は TLS のもとで利用できるものの、これは推奨される方法ではない。かわりに、 OAUTH2 のような、トークンベースの認証方式の利用を試みること。

IoT を安全に組織に導入するには、ここまでの IoT IAM ガイダンスに加え、以下の関連指針についても検討すること。

20 **“キルスイッチ”機能の必須化**。脆弱性が特定されているがアップデートやアップグレードが未提供の場合、“キルスイッチ”により IoT 管理者がデバイスのインターネット接続、LAN 接続、Bluetooth 接続を無効化できなければならない。また、配備される IoT システム毎の個別事情に応じ、IoT デバイスのファームウェアやソフトウェアの自動更新を有効にするかについても検討すること。

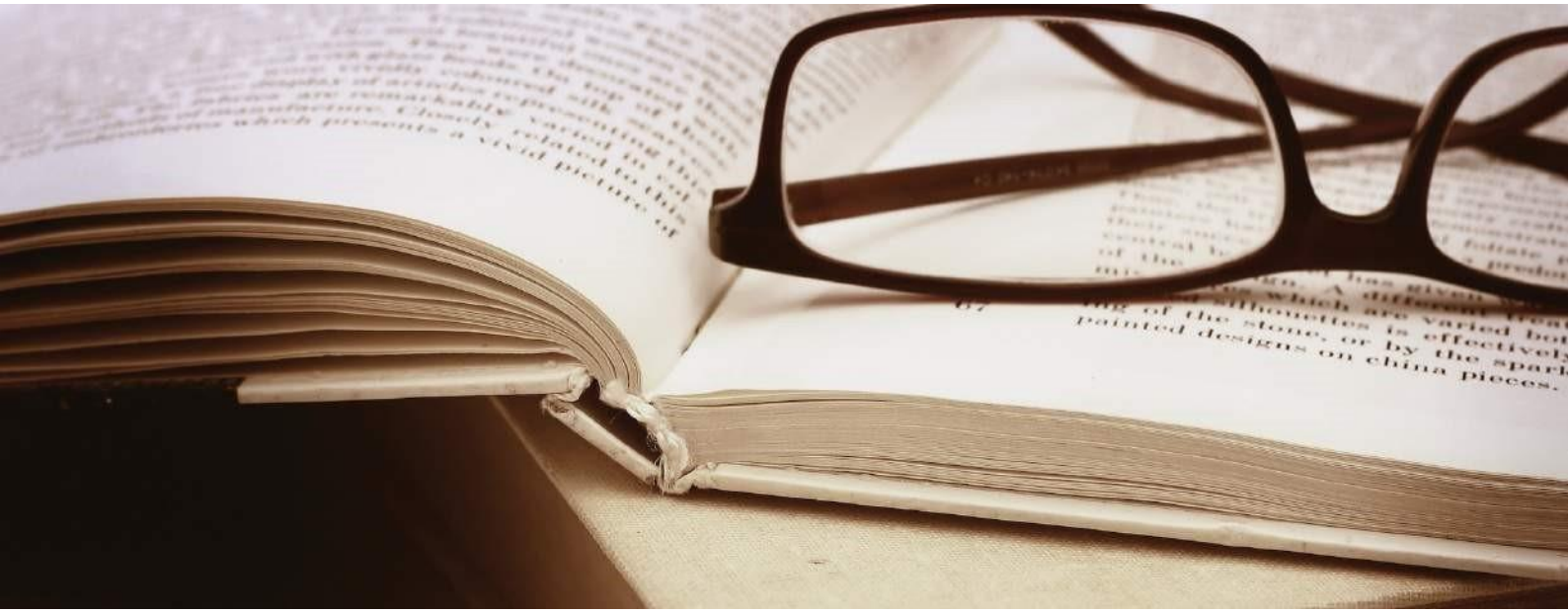
21 **利用者教育。**教育には以下の内容を含んでいる必要がある。

(1) ソフトウェア更新の必要性の確認方法
(2) 不具合が生じた場合にソフトウェア更新を元に戻す方法
(3) 他のデバイス（スマートフォン、無線ネットワーク、ビル管理システムネットワーク）のセキュリティがどのように IoT デバイスのセキュリティに影響を与えるか
(4) 顧客情報を保護し、プライバシーに関する設定を可能にするために必要な要件の理解

22 **安全なデフォルト設定を提供すること。**このように広い範囲に及ぶ利用者のためのセキュリティは可能な限りシンプルであるべきである。リセットボタンやリセット機能により自動的に最高レベルのセキュリティ設定が復元されなければならない。IoT デバイスのエンドユーザーは最低限のセキュリティについても意識できておらず、新たな機能により生じる脅威も存在しないものと考えている。望ましくない機能をブラックリスト化する代わりに、利用者がインパクトを理解しベネフィットを得られる機能をホワイトリスト化すべきである。

23 **IoT ユーザーの意識強化：**組織における IoT 利用によるデータの CIA（機密性、完全性、可用性）への影響について、IoT ユーザーに対し説明し認識してもらわなければならない。そのため、組織における IoT セキュリティを確保するためのベストプラクティスを促進するために啓発教育を設定すべきであり、以下のような事項を含めなければならない。

a. IoT セキュリティのための共通用語の定義
b. IoT 利用に関連するリスクの特定
c. IoT を保護するために配備された技術の解説
d. IoT デバイスを安全に利用するためのユーザー教育
e. その他



参考資料

"Things" will force makeover of enterprise ID, access management by John Fontana @ http://www.zdnet.com/article/things-will-force-makeover-of-enterprise-id-access-management/

Deploy360@IETF92, Day 2: DNSSEC, DANE, IPv6, IoT and Homenet @ http://www.internetsociety.org/deploy360/blog/2015/03/deploy360ietf92-day-2/

Challenges from the Identities of Things by Ingo Friese, Jorg Heuer and Ning Kong @ file:///C:/Users/Brian/Downloads/PID3057147.pdf

Managing the Authorization to Authorize in the Lifecycle of a Constrained Device @ https://datatracker.ietf.org/doc/draft-gerdes-ace-a2a/?include_text=1

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS (ITU-T Y.2060) @ https://www.itu.int/rec/T-REC-Y.2060-201206-I

10th Meeting of the Internet of Things Expert Group, report by Tom Wachtel @ http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7598&no=6

Expert Group on the Internet of Things (IoT-EG) @ http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752

The shift from IAM to Identity Relationship Management by Joni Brennan, Kantara Initiative @ http://www.scmagazine.com/the-shift-from-iam-to-identity-relationship-management/article/338758/

Gartner Says Managing Identities and Access Will Be Critical to the Success of the Internet of Things @ http://www.gartner.com/newsroom/id/2985717

Bluetooth SIG, FIDO collaboration could bring better security to Internet of Things by Monica
Alleven @ http://www.fiercewireless.com/tech/story/bluetooth-sig-fido-collaboration-could-bring-bettersecurity-internet-thing/2015-07-26

Identity Relationship Management by Kantara Initiative @ https://kantarainitiative.org/irmpillars/