AWS による IoT (モノのインターネット) のセキュリティ保護

セキュアなクラウドの採用

2019 年 4 月

注意

本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

目次

目的

このホワイトペーパーでは、AWS Cloud で使用できるセキュリティ保護対応の IoT (モノのインターネット) サービスについて詳述しています。このホワイトペーパーの想定読者は、IoT ソリューションを企業全体でセキュアに採用することを検討しているシニアレベルのプログラムオーナー、意思決定者、およびセキュリティ業務実施者です。

背景

IoT テクノロジーによってさまざまな形でプロセスの最適化、製品機能の充実、および顧客体験の変革を実現できるようになりました。このテクノロジーによって享受できるビジネスメリットにビジネスリーダーが大きな期待を抱いている一方で、セキュリティ、リスク、およびプライバシーに対する懸念は残ったままです。その一因として、異機種および非互換への対応が難しいことや、場合によっては適切でセキュアな展開が難しい未熟なセキュリティ機能しか用意されていないことが挙げられます。このような状況では、お客様または事業主のデータに関するリスクは高くなってしまいます。

人々の生活の質、事業運営とインテリジェンス、サービス提供者による介護の質、スマートシティのレジリエンス、環境の持続可能性、さらに現時点では想定されていない多くのシナリオを大幅に改善するスマートなサービスについて、さまざまな組織が意欲的に提供しようとしています。AWS では最近、ヘルスケア部門や地方自治体での IoT 採用事例が増加しており、近い将来、その他の業界も追随していくと予想されています。次に示すように、多くの自治体が IoT のような最新のテクノロジーをいち早く取り入れて先導的な役割を果たしています。

- **ミズーリ州カンザスシティ :** カンザスシティでは、新しく統合スマートシティプラットフォームのシステムを整備して、KC Streetcar (路面電車) の線路を管理しています。ビデオセンサー、路面センサー、ネットワークに接続された街灯、公開された WiFi ネットワーク、駐車場および交通量の管理によって、エネルギーコストの 40% 削減、17 億ドルもの都心部での新規開発効果、および 3,247 戸の新規住宅建設につながりました。
- **イリノイ州シカゴ市 :** シカゴでは交差点にセンサーとカメラを設置し、市民のために花粉の量と大気の状態を検知しています。
- **イタリア、カターニア市 :** カターニアでは、通勤者が目的地に向かう途中で、最も近くて空いている駐車場がどこかを確認できるアプリケーションを開発しました。
- **ブラジル、レシフェ市 :** レシフェでは、すべてのごみ収集トラックと清掃車に追跡装置を取り付けています。同市では、サービスの信頼性と運用効率を向上させながら、清掃費用を月当たり 25 万ドル削減しました。
- **英国、ウェールズのニューポート市 :** ニューポートでは、大気の状態、治水、および廃棄物管理を改善するために、スマートシティ IoT ソリューションをわずか数か月で展開しました。
- **インドネシア、ジャカルタ :** 洪水に頻繁に悩まされ、2800 万人の人口を抱える都市のジャカルタでは、IoT を活用して運河や低地の水位を検知したり、ソーシャルメディアを使用して市民の心理を追跡したりしています。また、対象とする地域に早期に警報と避難指示を発表し、最も支援が必要な地域を政府と初期対応部門が把握して避難プロセスを調整できています。

Machina Research によると、世界の IoT 市場規模は 2024 年までに 4 兆 3000 億ドルに達すると予想されています。[1] 英国のビジネス・イノベーション・技能省のレポートによると、スマートシティソリューションおよびその展開に必要な追加サービスの世界市場規模は 2020 年までに 4080 億ドルに達します。[2] さらに、Forbes[3] は、予知保全、自己最適化生産、および自動在庫管理が 2020 年までの IoT 市場の成長を牽引するユースケースの三本柱となると予想しています。Forbes は、IoT ソリューションを構築または展開する場合の影響の大きさから、IT ベンダーを選択する際には信頼性の高いインフラストラクチャを持ち、実績があり、成熟した IT ベンダーを希望している企業が多いと述べています。

顧客は IoT を通じて利用可能となるビジネスチャンスを活用することに大きな期待を寄せていますが、これまでのところ、IoT 採用時の安全面については不安がつきまとっていました。ソリューションを可能にする機能やサービスは、デフォルトのままでは必ずしも安全ではなく、アーキテクチャの基盤にも潜在的なセキュリティギャップが残されたままでした。さらに、暗号化通信、無線による (OTA) 更新などの重要な機能の更新とメンテナンスは自動実行ではありませんでした。また、デバイスとゲートウェイにリモートでパッチを適用する機能をサービスの展開後に引き続きサポートしているプロバイダはほとんどなく、パッチの適用されていないデバイスは新たなセキュリティリスクの影響を受けやすくなっていました。

これとは対照的に、AWS はセキュリティを非常に重視しており、幅広い業界や地域で何百万ものアクティブな顧客のデータの機密性や機密保持の多岐にわたる要件をサポートしています。AWS は、非常に多くのリソースを投入し、サービスのすべてのレイヤーにセキュリティを確実に組み込んで、IoT を備えたデバイスにセキュリティを拡張しています。AWS の優先事項は、IoT ソリューションに向けて安全で拡張性が高く、セキュアなプラットフォームを提供しながら、顧客のシステムとデータの機密性、完全性、可用性を確保することです。

セキュリティの課題

セキュリティリスクと脆弱性によって、IoT アプリケーションで使用される顧客データのセキュリティとプライバシーが侵害される可能性があります。デバイスの数や生成されるデータの増加と相まって、IoT デバイスそのもの、およびクラウドとのデバイス間通信がもたらすセキュリティリスクへの対処方法について疑問が投げかけられています。

リスクに関するお客様の懸念に共通するのは、デバイスへのパッチ適用、デバイスとユーザーの認証、およびアクセスコントロール時に発生するクラウドまたはエッジサービスとデバイス間の転送データのセキュリティと暗号化です。IoT デバイスのセキュリティは、データの完全性を維持するためだけでなく、デバイスの信頼性に影響を与える可能性のある攻撃から保護するためにも不可欠です。デバイスは大量の機密データをインターネット経由で送信でき、エンドユーザーはデバイスを直接制御できるため、「モノ」のセキュリティをソリューションのすべてのレイヤーで浸透させる必要があります。

度重なるデータ侵害の報道によって IoT セキュリティは顧客のさらなる監視下に置かれていますが、そこから得られた教訓はベストプラクティスに近付けるための取り組みに生かされています。IoT ソリューションの基盤は、セキュリティに始まり、セキュリティに

---

1 https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024 を参照してください。

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217-smart-city-market-opportunties-uk.pdf を参照してください。

3 https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#74c8f8c7609b を参照してください。

終わります。すなわち、IoT のコンフィギュレーション[4] を継続的に監査できるサービスを使用してセキュリティのベストプラクティスから逸脱しないようにしつつ、逸脱が検出された場合は、適切な是正措置を実行できるように、アラートを (理想としては、自動的に) 生成する必要があります。

市場へのデバイスの投入とオンラインからの脅威への対応を同時に実現するには、IoT エコシステムの各部分に対応しつつ、(クラウドとの接続の有無に関わらず) セキュリティと保護、監査と是正、および IoT デバイスの展開管理を行う機能がそれぞれの領域と重なる部分を持つよう設計されたサービスを実装するのが最適です。

IoT セキュリティに対する政府の取り組み

民間部門の組織がヘルスケア、産業向け建設、低電力消費財などのユースケースで IoT を積極的に展開している中、国や地方レベルの政府も IoT の採用とセキュリティに取り組み始めています (付録 2 を参照)。IoT に関する政策の将来展望を評価することに加えて、さまざまなコンプライアンスフレームワークにサービスを追加しながら、お客様がコンプライアンス義務 (付録 3 を参照) を果たせるよう支援していきます。

AWS IoT サービスとセキュリティ機能

AWS は IoT サービスのスイート製品を提供し、お客様のデバイス、接続性、およびデータのセキュリティ保護を支援します。このようなサービスにより、デバイスの保護から転送中および保管時のデータに至るまでのエンドツーエンドのセキュリティ機能を活用できます。また、セキュリティウォーターマークを満たすために必要なセキュリティポリシーの適用と実行を可能にするセキュリティ機能も提供されています。

AWS IoT は幅広い機能を提供しています。お客様はさまざまなデバイスのあらゆるユースケースに対応する IoT ソリューションを構築できます。AWS IoT は人工知能 (AI) サービスと統合されているため、インターネットに接続しなくてもデバイスをよりスマートにすることができます。AWS IoT は AWS クラウドに構築され 190 か国の何百万ものお客様によって使用されており、お客様のデバイス数の増加およびビジネス要件の進化に合わせて容易に拡張できます。AWS IoT は包括的なセキュリティ機能も提供しているため、お客様は予防的なセキュリティポリシーを作成して潜在的なセキュリティ問題に即座に対応できます。

AWS IoT はクラウドサービスとエッジソフトウェアを提供しており、インターネット接続がダウンしていてもセキュアにデバイスに接続してデータを収集し、デバイス内でインテリジェントなアクションを実行できます。クラウドサービスを利用することで、展開された多種多様なデバイスに迅速かつセキュアに接続して、デバイスの健全性と安全性を維持しながら IoT のセンサーやアプリケーションにまたがるイベントを検知して対応することができます。IoT アプリケーションの開発を促進するために、お客様はドラッグアンドドロップインターフェースを使用してデバイスとウェブサービスを簡単に接続することができます。AWS IoT を使用して、データを分析し、高度な機械学習 (ML) モデルを構築することもできます。そのようなモデルをクラウドやお客様のデバイスに展開することで、デバイスをよりスマートにすることができます。

4　コンフィギュレーションとは、デバイスが相互に通信したり、クラウドと通信したりする際に、情報のセキュリティを維持するためにお客様が設定する一連の技術的な規制です。

現在の AWS IoT サービス [5] は革新的で包括的な IoT ソリューションを実現するために幅広く使われていますが、このホワイトペーパーでは、IoT セキュリティの基礎となる次の 5 つのサービスを重点的に取り上げます。サービスの説明とセキュリティ機能については、後で詳しく説明します。

- **Amazon FreeRTOS** は、マイクロコントローラー用のオープンソースオペレーティングシステムで、小型かつ低消費電力のエッジデバイスのプログラミング、展開、セキュリティ保護、接続、および管理を容易にします。
- **AWS IoT Greengrass** は、接続されたデバイスでローカルコンピューティング、メッセージング、データキャッシング、同期、および ML 推論機能を実行できるソフトウェアです。
- **AWS IoT Core** は、接続されたデバイスが簡単かつセキュアにクラウドアプリケーションおよびその他のデバイスと情報を交換できるようにするマネージドクラウドサービスです。
- **AWS IoT Device Management** は、IoT デバイスの大規模な実装、整理、監視、およびリモート管理をセキュアに行うことができるクラウドベースのデバイス管理サービスです。
- **AWS IoT Device Defender** は、お客様の IoT コンフィギュレーションを継続的に監視および監査して、セキュリティのベストプラクティスから逸脱していないことを保証する IoT セキュリティサービスです。

Amazon FreeRTOS – デバイスソフトウェア

サービスの概要： Amazon FreeRTOS (a:FreeRTOS) は、マイクロコントローラー用のオープンソースオペレーティングシステムで、[6] 小型かつ低消費電力のエッジデバイスのプログラミング、展開、セキュリティ保護、接続、および管理を容易にします。Amazon FreeRTOS は、マイクロコントローラー向けに幅広く使用されているオープンソースオペレーティングシステムである FreeRTOS カーネルをベースにソフトウェアライブラリを拡張しています。これにより、AWS IoT Core などの AWS Cloud サービスや AWS IoT Greengrass が稼働する強力なエッジデバイスにお客様の小型かつ低消費電力のデバイスを安全に直接接続できるようになります。

セキュリティ機能： Amazon FreeRTOS には、データ暗号化とキー管理のサポートを含む、デバイスのデータと接続を保護するライブラリが付属しています。Amazon FreeRTOS は Transport Layer Security (TLS v1.2) をサポートし、デバイスがクラウドにセキュアに接続できるようにしています。Amazon FreeRTOS には、お客様のデバイスコードが展開中に侵害されていないことを保証するコード署名機能に加え、機能強化またはセキュリティパッチでデバイスをリモート更新する OTA 更新機能もあります。

5　AWS IoT サービスには、Amazon FreeRTOS、AWS IoT Greengrass、AWS IoT Core、AWS IoT Device Management、AWS IoT Device Defender、AWS IoT Things Graph、AWS IoT Analytics、AWS IoT SiteWise、AWS IoT Events が含まれています。詳細については、https://aws.amazon.com/iot を参照してください。

6　マイクロコントローラーは、電化製品、フィットネストラッカー、産業用オートメーションセンサー、自動車など、多くのデバイスに搭載されている単純なプロセッサを含む単一のチップです。このような小型デバイスの多くは、クラウドに接続したり、現場で他のデバイスに接続したりすることでメリットを享受できます。たとえば、スマート電気メーターは使用状況を報告するためにクラウドに接続する必要があります。また、担当者が現場でデバイスへのアクセスを要求した際に、ドアのロックが解除されるような通信を行うためのセキュリティシステムを構築する必要があります。

AWS IoT Greengrass – エッジコンピューティングのためのソフトウェア

サービスの概要： AWS IoT Greengrass は、接続されたデバイスに対して、ローカルコンピューティング、メッセージング、データキャッシング、同期、および ML 推論機能を実行できるソフトウェアであり、[7] クラウドへの接続が断続的な場合でも接続されたデバイスを動作させることができます。デバイスが再接続されると、AWS IoT Greengrass はデバイスのデータを AWS IoT Core と同期させ、接続の状況に関係なく一定の機能を提供します。AWS IoT Greengrass は AWS からデバイスへのシームレスな拡張を提供するため、デバイスで生成されたデータをローカルで処理しながら、クラウドを管理、分析、および耐久性のあるストレージとして使用できます。

セキュリティ機能： AWS IoT Greengrass は、現場での通信とクラウドとの通信の両方でデバイスデータを認証し、暗号化します。証明された ID がない場合、データがデバイス間やクラウドとの間で送受信されることはありません。このサービスでは、相互デバイス認証および承認、クラウドへのセキュアな接続とともに、AWS IoT Core でお客様が慣れ親しんでいるものと同様のセキュリティとアクセス管理を使用しています。

具体的には、AWS IoT Greengrass は、X.509[8] 証明書、マネージドサブスクリプション、AWS IoT ポリシー、AWS Identity and Access Management (IAM) ポリシーおよびロールを使用して、AWS IoT Greengrass アプリケーションの安全性を確保しています。AWS IoT デバイスが AWS IoT Greengrass サービスに接続するには、AWS IoT Thing、デバイス証明書、および AWS IoT ポリシーが必要になります。これにより、AWS IoT Greengrass コアデバイスは AWS IoT クラウドサービスにセキュアに接続できるようになります。また、この接続によって、AWS IoT Greengrass クラウドサービスがコンフィギュレーション情報、AWS Lambda 機能、およびマネージドサブスクリプションを AWS IoT Greengrass コアデバイスに展開できるようになります。さらに、AWS IoT Greengrass は、エッジデバイスのための信頼されたプライベートキーストレージのハードウェアルートを提供します。

AWS IoT Greengrass のその他の重要なセキュリティ機能は、監視とロギングです。たとえば、このサービスのコアソフトウェアは、Amazon CloudWatch[9] (AWS IoT Core にも対応しています) やお客様のコアデバイスのローカルファイルシステムにログを書き込むことができます。ロギングはグループレベルで設定され、すべての AWS IoT Greengrass ログエントリにはタイムスタンプ、ログレベル、およびイベントに関する情報が含まれます。AWS IoT Greengrass は AWS CloudTrail[10] (AWS IoT Greengrass でのユーザー、ロール、または AWS のサービスによるアクションの記録を提供するサービス) と統合されています。お客様が CloudTrail をアクティブ化すると、AWS IoT Greengrass に対するすべてのアプリケーションプログラミングインターフェース (API) 呼び出しが収集されます。収集結果には、AWS IoT Greengrass コンソールからの呼び出し、および AWS IoT Greengrass API 操作に対するコード呼び出しが含まれます。たとえば、お客様がトレイルを作成すると、呼び出しによって AWS IoT Greengrass のイベントを含む AWS CloudTrail のイベントを Amazon Simple Storage Service (Amazon S3) バケットに継続的に配信することが

---

7 AWS IoT Greengrass を使用するには、AWS IoT Greengrass のコアを動かすことができるデバイスが必要になります。認定されたデバイスと技術的な依存関係の完全なリストを確認するには、こちらをクリックしてください。実践的な入門ガイドについては、こちらをクリックしてください。詳細な開発者向けリファレンスについては、こちらをクリックしてください。

8 X.509 証明書は、X 509 公開鍵インフラストラクチャ標準を使用して公開鍵を証明書に含まれる ID に関連付けるデジタル証明書です。X.509 証明書は、証明機関 (CA) と呼ばれる信頼された事業体によって発行されます。CA は、X.509 証明書を発行するために使用する CA 証明書と呼ばれる 1 つ以上の特殊な証明書を保持します。CA 証明書にアクセスできるのは、認証機関だけです。詳細については、https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html を参照してください。

9 https://aws.amazon.com/cloudwatch を参照してください。

10 https://aws.amazon.com/cloudtrail を参照してください。

できます。トレイルを作成したくない場合、AWS CloudTrail コンソールの最新のイベントをイベント履歴で確認できます (有効になっている場合)。この情報は、AWS IoT Greengrass へのリクエストが行われた時刻やリクエスト元の IP アドレスの確認など、さまざまな用途に利用できます。

デバイスにあるお客様のデータのセキュリティを保護するためのベストプラクティスオプションが用意されており、可能な場合は常に使用されます。AWS IoT Greengrass では、すべての IoT デバイスがフルディスク暗号化を有効にし、キー管理のベストプラクティスに従います。NIST FIPS 140-2 で検証済みのアルゴリズム [11] に基づく AES256 ビットキーを使用したフルディスク暗号化を利用すると、キー管理のベストプラクティスに準拠できます。Amazon FreeRTOS を使用しているような低電力デバイスでは NIST 8114 の軽量暗号 [12] の推奨事項に準拠できます。

上記のセクションでは、マイクロコントローラーとエッジのユースケースについて説明しました。下記では、クラウドで動作する IoT サービスを重点的に取り上げます。

AWS IoT Core – クラウドベースの IoT ゲートウェイ

サービスの概要 : AWS IoT Core は、接続されたデバイスが簡単かつセキュアにクラウドアプリケーションおよびその他のデバイスと情報を交換できるようにするマネージドクラウドサービスです。AWS IoT Core は、接続された多様なデバイスおよびさまざまな場所の間で安全な通信とデータ処理を提供するので、IoT アプリケーションを簡単に構築できます。ユースケースの例として、産業向けのソリューションやコネクテッドホームソリューションがあります。何十億台ものデバイスや何兆個ものメッセージをサポートし、これらを処理して AWS エンドポイントとその他のデバイスに確実かつセキュアにルーティングできます。

セキュリティ機能 : AWS IoT Core は、セキュリティの実現と維持を支援する多数のソリューションをユーザーに提供します。AWS Cloud セキュリティメカニズムによって、AWS IoT と、その他のデバイスや AWS のサービスとの間を移動するデータが保護されます。デバイスは、セキュアな接続を介して、さまざまな ID オプション (X.509 証明書、IAM ユーザーおよびグループ、Amazon Cognito ID、またはカスタム認証トークン) を使用して接続できます。お客様がクライアントサイド検証 (一連の信頼性検証、ホスト名検証、セキュアなストレージ、およびプライベートキーの配布) を行うと、AWS IoT Core からは TLS を使用したセキュアな転送チャネルが提供されます。AWS IoT ルールエンジンは、お客様が定義するルールに従ってデバイスデータを他のデバイスや AWS のサービスに転送します。AWS アクセス管理システムは、データを最終的な転送先までセキュアに転送するために使用されます。注目すべき AWS IoT のもう 1 つの認証機能として、AWS IoT のポリシー変数があります。このポリシー変数によって、過剰な特権を伴う認証情報がプロビジョニングされることを防止します。このような機能は、一般的なサイバーセキュリティのベストプラクティスと組み合わせて使用され、お客様のデータの保護に役立ちます。

---

11 NIST FIPS 140-2 で承認済の暗号化アルゴリズム : https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.

12 NIST 8114 – 軽量暗号 : https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

AWS IoT Device Management – クラウドベースの IoT デバイス管理サービス

サービスの概要 : AWS IoT Device Management は、IoT デバイスの大規模な実装、整理、監視、およびリモート管理を支援します。AWS IoT Device Management は AWS IoT Core と統合されており、デバイスをクラウドおよびその他のデバイスと簡単に接続できるため、お客様は展開したデバイスをリモートで管理できます。AWS IoT Device Management は、AWS Management Console 内の AWS IoT または API を使用して、デバイスのメーカーおよびシリアル番号、X.509 ID 証明書、セキュリティポリシーなどの情報を入力するテンプレートをアップロードすることで、新たなデバイスの実装を支援します。その後、お客様は AWS Management Console 内で AWS IoT を数回クリックするだけで、そのような情報を使用して展開したデバイス全体を構成できます。

セキュリティ機能 : AWS IoT Device Management を使用すると、展開したデバイスの階層構造を機能やセキュリティ要件などのカテゴリに基づいて作成できます。たとえば、1 つの部屋にある 1 つのデバイス、同じフロアにある複数のデバイス、または 1 つの建物内で動作しているすべてのデバイスをグループ化できます。このようなグループを使用すると、アクセスポリシーの管理、運用メトリックの表示、グループ全体でのアクションの実行が可能になります。さらに、「Dynamic Things」と呼ばれる機能により、お客様が定義した基準を満たすデバイスを自動的に追加し、要件を満たさなくなったデバイスを削除できます。これにより、運用の完全性を維持しながら、プロセスをセキュアに合理化できます。また、Dynamic Things 機能によって、デバイス属性の任意の組み合わせに基づいてデバイスレコードを簡単に特定し、一括更新を実行できます。

AWS IoT Device Management を使用することにより、ソフトウェアとファームウェアを現場のデバイスにプッシュして、セキュリティの脆弱性にパッチを当て、デバイスの機能を改善することもできます。また、一括更新の実行、展開速度の制御、および障害しきい値の設定を実施したり、常に最新バージョンが実行されるように、デバイスのソフトウェアを自動的に更新する継続的なジョブを定義したりすることもできます。デバイスの再起動、工場出荷時設定へのリセットなどの処理をリモートで送信して、デバイスのソフトウェアの問題を修正したり、デバイスの元の設定を復元したりすることができます。また、デバイスに送信されるファイルにデジタル署名を付け、デバイスのセキュリティ侵害を防止できます。

ソフトウェア更新をプッシュできるのはクラウドサービスだけではありません。Amazon FreeRTOS の OTA 更新ジョブを使用すると、お客様は AWS IoT Device Management を利用してソフトウェア更新をスケジュールできます。同様に、接続されたデバイスにセキュリティ更新、バグ修正、および新しい AWS IoT Greengrass 機能を展開するために、AWS IoT Device Management を使用して 1 つ以上の AWS IoT Greengrass コアデバイス向けの AWS IoT Greengrass コア更新ジョブを作成できます。

AWS IoT Device Defender – クラウドベースの IoT デバイスセキュリティサービス

サービスの概要 : AWS IoT Device Defender はフルマネージドサービスであり、展開された IoT デバイス向けに確立されたセキュリティ機能をお客様が監査する際に役に立ちます。このサービスは、IoT コンフィギュレーションを継続的に監査して、IoT コンフィギュレーションを維持および実装するためのセキュリティのベストプラクティス (デバイス ID の保証、デバイスの認証と承認、デバイスデータの暗号化など) からコンフィギュレーションが逸脱していないことを確認します。また、ID 証明書が複数のデバイス間で共有されている場合や、失効した ID 証明書を伴うデバイスが AWS IoT Core に接続しようとした場合など、セキュリティリスクを引き起こす可能性のあるギャップがお客様の IoT コンフィギュレーションにある場合、アラートを送信できます。

セキュリティ機能：サービスの監視機能および監査機能に加えて、お客様が設定したアラートを使用してデバイスで検出された逸脱を是正するアクションを実行できます。たとえば、アウトバウンドトラフィックにあるスパイクは、デバイスが分散型サービス拒否 (DDoS) 攻撃に加担している可能性を示します。AWS IoT Greengrass と Amazon FreeRTOS は、AWS IoT Device Defender とも自動的に統合され、評価のためにデバイスから取得したセキュリティメトリクスを提供します。

AWS IoT Device Defender によって、AWS IoT、Amazon CloudWatch、および Amazon Simple Notification Service (Amazon SNS) にアラートを送信可能で、アラートは Amazon CloudWatch メトリクスに公開されます。お客様がアラートに対処する場合、AWS IoT Device Management を使用して、セキュリティ修正コードのプッシュなどの軽減措置を取ることができます。

AWS IoT Device Defender が、定義された一連の IoT セキュリティベストプラクティスと照らし合わせて、お客様のデバイスに関連する IoT コンフィギュレーションを監査するので、お客様はセキュリティギャップの存在場所を確認し、継続的な監査や一時的な監査を実行できます。AWS IoT Device Defender には、監査の一環として選択および実行可能なセキュリティプラクティスもあります。このサービスは Amazon CloudWatch、Amazon SNS などの他の AWS のサービスとも統合されており、監査が失敗した場合や挙動の異常が検出された場合、セキュリティアラートを AWS IoT に送信し、お客様が根本原因を調査して判断できるようにしています。たとえば、AWS IoT Device Defender は、デバイス ID が機密性の高い API にアクセスしている場合にお客様にアラートを送付できます。AWS IoT Device Defender は、許可の取り消し、デバイスの再起動、工場出荷時のデフォルト設定へのリセット、お客様が接続しているデバイスへのセキュリティ修正コードのプッシュなど、セキュリティ問題の影響を最小限に抑えるアクションを推奨することもできます。

人為的またはシステム的なエラーや悪意を持つ認証済みユーザーによってセキュリティに悪影響を与えるコンフィギュレーションが導入されてしまうことを懸念もあります。AWS IoT Core では、お客様がデバイスをクラウドおよびその他のデバイスとセキュアに接続するためのセキュリティ構成ブロックを提供しています。構成ブロックを使用することで、認証、許可、監査ログ、エンドツーエンド暗号化などのセキュリティ制御を実行できます。これにより、AWS IoT Device Defender の介入が可能になり、セキュリティのベストプラクティスとお客様独自の組織的なセキュリティポリシーに準拠するためのセキュリティコンフィギュレーションの継続的な監査を支援できます。

IoT を強化するための証明可能安全性の活用 – 業界の差別化要素

AWS では、企業が IoT とエッジデバイスのセキュリティを確保できるようにセキュリティに関する新たなサービスやテクノロジーの構築が継続的に実施されています。AWS では最近、自動推論として知られる AI テクノロジーを利用した AWS IoT Device Defender 内のチェックを開始しました。このテクノロジーでは数学的証明を活用して、ソフトウェアが正しくコーディングされているかどうかを検証し、デバイスへの意図せぬアクセスがないかどうかも判断しています。AWS IoT Device Defender は、お客様が自動推論を直接使用して、所有するデバイスを保護する方法の一つになります。内部的には自動推論を使用して、Amazon FreeRTOS で動作するコードのメモリ完全性を検証し、マルウェアから保護しています。セキュアなソフトウェアによる拡張可能な保証 (「証明可能安全性」と呼ばれます) を提供する自動推論に投資すると、お客様は AWS で機密性の高いワークロードを操作できるようになります。

AWS Zelkova[13] は自動推論を使用して、お客様のデータアクセスコントロールが意図したとおりに機能していることを証明します。AWS IoT Device Defender でのアクセスコントロールチェックには Zelkova が利用されており、お客様はデータが適切に保護されていることを確認できます。AWS IoT ポリシーは、お客様が意図したセキュリティコンフィギュレーションの対象ではないリソースへアクセスを許可する場合、許容度が広すぎます。AWS IoT Device Defender に組み込まれた Zelkova ベースのコントロールは、お客様のセキュリティコンフィギュレーションによって制限されたアクションがポリシーによって許可されていないこと、意図したリソースに特定のアクションを実行する権限が与えられていることを検証します。

その他の自動推論ツールも、AWS IoT インフラストラクチャの安全性を向上させるために使用されています。オープンソースの標準的な検証ツール CBMC が AWS IoT インフラストラクチャの基盤を強化するために使用されており、Amazon FreeRTOS オペレーティングシステムの重要なコンポーネントに対するメモリの安全性を証明しています。メモリの安全性を証明することで、特定のセキュリティ問題の可能性は最小限に抑えられ、その結果、お客様と開発者は環境内の他の領域のセキュリティ保護に集中できます。メモリの安全性の証明は、Amazon FreeRTOS のコードが変更されるたびに自動的にチェックされ、お客様と AWS 開発者の両方に対し、重要なコンポーネントのセキュリティに関する信頼性を継続的に維持しています。

AWS では、自動推論の実装をさまざまな AWS のサービスや機能で継続し、AWS Cloud の重要なコンポーネントに対する高度なセキュリティ保証を提供します。また、AWS IoT スタックのための内部インフラストラクチャ検証テクノロジーだけでなく、お客様のためのツールを開発する際にも自動推論を採用しています。

IoT セキュリティの重要なベストプラクティス

利用可能なベストプラクティスは数多く存在しますが、IoT ソリューションのリスクを軽減するための万能なアプローチは存在しません。デバイス、システム、およびサービスによって、さらにはデバイスが展開されている環境によって、お客様が考慮すべき脅威、脆弱性、およびリスク許容度は異なります。データ、デバイス、およびクラウドサービスにエンドツーエンドセキュリティを組み込む際の推奨事項を次に示しています。

1. **設計フェーズでのセキュリティの組み込み**
   IoT ソリューションの基盤はセキュリティに始まり、セキュリティに終わります。デバイスが大量の機密データを送信する可能性があり、IoT アプリケーションのエンドユーザーもデバイスを直接制御する可能性があるため、「モノ」のセキュリティの設計要件は必然的に広範なものとなります。セキュリティは固定的な手段ではありません。IoT アプリケーションを使用する際には、セキュリティのベストプラクティスを継続的にモデル化、監視、および反復できることを考慮に入れる必要があります。IoT セキュリティの課題とは、物理デバイスのライフサイクルであり、センサー、マイクロコントローラー、アクチュエータ、組み込みライブラリに対するハードウェアの制約です。このような制約要素により、個々のデバイスが実行できるセキュリティ機能が制限される場合があります。IoT ソリューションでは、変化するセキュリティ環境で先端を行くために、日々変動する要因に対応してアーキテクチャ、ファームウェア、およびソフトウェアを継続的に適応させる必要があります。デバイスの制約要素により、リスク、障害、セキュリティとコスト間のトレードオフが増える可能性がありますが、どのような組織にとってもセキュアな IoT ソリューションを構築することが重要な目標であることに変わりはありません。

---

13 Zelkova の詳細については、https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated-reasoning-zelkova を参照してください。

2. **広く認められた IT セキュリティおよびサイバーセキュリティフレームワークに基づいた構築**
   AWS はオープンな標準ベースのアプローチをサポートして、セキュアな IoT の採用を促進しています。消費者、産業、および公共部門向けの堅牢な IoT エコシステムをサポートするための必要な数十億ものデバイスと接続ポイントを考慮する際に、相互運用性は不可欠です。そのため、AWS IoT サービスは業界標準のプロトコルとベストプラクティスに準拠しています。さらに、AWS IoT Core は他の業界標準プロトコルとカスタムプロトコルもサポートしているので、異なるプロトコルを使用しているデバイス同士でも通信が可能です。AWS は相互運用性を強力に支持しているため、開発者は既存のプラットフォームの最上層をベースとして、進化する顧客ニーズへの対応を進めることができます。また、AWS は広範なパートナーエコシステムをサポートしているので、選択の幅が広がり、お客様の可能性の限界もさらに広がります。世界的に認められたベストプラクティスを適用することで、IoT のすべての利害関係者は次のような多くのメリットを享受できます。

   - 再始動と再実行ではなく、繰り返し適用と再利用
   - 地理的境界を越えるテクノロジーの互換性と相互運用性を促進する一貫性とコンセンサス
   - IT への最新テクノロジーの応用と変革を促進する効率性の最大化

3. **セキュリティ対策の優先度付けに対する影響の検討**
   攻撃や異常にまったく同じものは存在せず、対象が人、業務、およびデータであるかによって影響も異なります。お客様の IoT エコシステムとそのエコシステム内でデバイスが動作する場所を理解すると、最も大きいリスクが、ネットワークの一部としてのデバイスか、物理的なコンポーネントあるいはセキュリティのうちのどこにあるかを判断できます。IoT エコシステムにおいてセキュリティの取り組みをどこで実施すべきで、誰がそのような取り組みの責任を担うかを決定する際には、リスク影響評価とその結果に重きを置くことが不可欠です。

まとめ

IoT の「モノ」は、接続されるデバイスの急激な増加に伴い、信頼性の高い接続性、ストレージ、およびセキュリティを必要とするデータのパケットを送受信するようになっています。IoT を利用すると、分散したデバイスから送られる大量のデータとそれぞれの接続を管理および監視して、さらにそのセキュリティも保護する必要があるという課題に直面します。しかし、この課題は必ずしもクラウドベースの環境で障害になるわけではありません。クラウドコンピューティングでは、1 つのソリューションを 1 つの場所で拡張および強化できるだけでなく、複数の IoT ソリューションを物理的に異なる場所からグローバルに拡張して、通信レイテンシーを短縮し、現場のデバイスからの応答性を向上させることができます。AWS では、エンドポイント、ゲートウェイ、プラットフォーム、アプリケーション、さらにはこのようなレイヤーを横断するトラフィックの運用とセキュリティ保護を行うサービスを含む、エンドツーエンドのセキュリティを備えた IoT サービスのスイート製品を提供しています。これらを使用した統合により、セキュリティを優先事項として維持しながら、継続的に影響し合うデバイスとデータの安全な使用と管理を簡素化でき、IoT によって実現されるイノベーションと効率性のメリットを享受できます。

付録 1 – AWS IoT サービスの統合

AWS IoT は、次の AWS のサービスと直接統合されています。

- **Amazon Simple Storage Service (Amazon S3)** は、AWS Cloud でスケーラブルなストレージを提供します。詳細については、Amazon S3 を参照してください。
- **Amazon DynamoDB** はマネージド NoSQL データベースを提供します。詳細については、Amazon DynamoDB を参照してください。
- **Amazon Kinesis** は、大規模なストリーミングデータのリアルタイム処理を可能にします。詳細については、Amazon Kinesis を参照してください。
- **AWS Lambda** は、Amazon Elastic Compute Cloud (Amazon EC2) の仮想サーバーで、イベントに対応したお客様のコードを実行します。詳細については AWS Lambda を参照してください。
- **Amazon Simple Notification Service (Amazon SNS)** は、通知を送受信します。詳細については、Amazon SNS を参照してください。
- **Amazon Simple Queue Service (Amazon SQS)** は、アプリケーションが取得するデータをキューに格納します。詳細は、Amazon SQS を参照してください。

付録 2 – IoT に取り組む政府機関

米国

アメリカ国立標準技術研究所 (NIST) – 米国商務省

米国商務省は、IoT セキュリティに対処する複数の取り組みを先導しています。アメリカ国立標準技術研究所 (NIST) が発行したホワイトペーパー [14] では、データおよびデバイスのセキュリティを評価する際に、お客様と政府機関の両方が検討するトピックを明らかにしています。このホワイトペーパーでは、そのような懸念事項を評価するよう促し、問題の影響度を軽減するための推奨事項を提示しています。NIST は IoT の採用に悪影響を及ぼす可能性のあるリスクを特定した NIST Internal Report (NISTIR) 8228[15] も発表しました。また、この文書はそのような懸念の影響を緩和または低減するための推奨事項も提示しています。NIST は、数多くの取り組みの中でも、官民パートナーシップを招集し、コメントを求め、スマートシティと IoT の国際標準化に関するワークショップを主催しています。[16] 取り組みはまだ初期段階ですが、政府と消費者が IoT を通じて利用できる恩恵に対する深刻な課題として、サイバーセキュリティとプライバシーのリスクの可能性が指摘されています。

国防総省

政府での取り組みのもう 1 つの例は、国防分野に存在します。2016 年には、米国防総省 (DoD) の最高情報責任者が IoT の脆弱性とリスクに対処するための政策提言を行いました。[17] その政策提言よると、米国防総省はすでに数百万台の IoT デバイスとセンサーを国防総省の施設、車両、および医療機器に展開しており、兵器や情報機関向けシステムに組み込むことも検討しています。IoT セキュリティの複雑さは、デバイスの数が膨大であること、さらにはファイアウォールやマルウェア対策を実行するデバイスの処理能力が限られていることに起因しています。その結果、従来のモバイルデバイスとは異なるレベルの脆弱性が内在しています。

国防総省が IoT セキュリティリスクに対処するために推奨するアプローチと政策措置には、次の 3 点があります。1) 個々の IoT 実装とそれぞれに関連するデータストリームをサポートするセキュリティとプライバシーのリスク分析、2) コストがリスクと価値に見合うすべてのポイントでの暗号化、3) 異常トラフィックと差し迫った脅威を特定する IoT ネットワークの監視。

連邦取引委員会 (FTC)

FTC は IoT セキュリティに関する議論の重要な参加者であり、セキュリティに関する義務に関する虚偽または過失があったデバイスメーカーに対して訴訟を起こしています。FTC は「合理的なデータセキュリティ」の基準を定めています。FTC は、デバイスメーカーにおいて、次のようなセキュリティに関する欠陥が繰り返されていることを指摘しました。

---

14 Jeffrey Voas (NIST)、Richard Kuhn (NIST)、Phillip Laplante (ペンシルベニア州立大学)、Sophia Applebaum (MITRE) "Internet of Things (IoT) Trust Concerns" (2018 年 10 月 16 日、https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft)

15 NISTIR 8228、"Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment" (2018 年 9 月 26 日、https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy)

16 https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot を参照してください。

17 https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440 を参照してください。

- セキュリティがデバイスに組み込まれていない
- 開発会社が、適切なセキュリティプラクティスについて従業員を教育していない
- ダウンストリームセキュリティとコンプライアンスを (契約を用いて) 確保していない
- 多層防御戦略の欠如
- 合理的なアクセスコントロールの欠如 (顧客はデフォルトのパスワードを迂回または推測が可能)
- データセキュリティプログラムの欠如

カリフォルニア州

カリフォルニア州は米国で最初に IoT に関する法案を成立させた州です。現在の法案ではデバイス設計のセキュリティやデータ保護などの課題に言及していますが、IoT メーカーに特定の要件を課しているわけではありません。その代わり、議員たちは設計段階のセキュリティに重点を置き、データの保護は「装置の特質と機能に適合」していて、「収集、格納、または送信する情報に適合」していなければならないとしています。

英国

英国のデジタル・文化・メディア・スポーツ省 (DCMS) は、Code of Practice for Consumer IoT Security の最終版を 2018 年 10 月に公開しました。[18] この文書は、国家サイバーセキュリティセンター (NCSC) と共同で起草され、消費者団体、業界、学界からの意見を取り入れています。また、消費者向け IoT 製品の開発、製造、および販売に携わるすべての組織が「セキュア・バイ・デザイン」アプローチを実現する方法について、13 のガイドラインが記載されています。

さらに、ユーザーが最大限かつ即時にセキュリティに関するメリットを享受するための次のような 3 つの主要なプラクティスを強調し、IoT の利害関係者にこのようなプラクティスを優先するよう促しています。1) デフォルトパスワードなし : 多くのユーザーはデフォルトパスワードを変更しませんが、これは多くの IoT セキュリティ問題の原因となっています。2) 脆弱性開示ポリシーの実践 : IoT デバイス、サービス、およびアプリ開発者は、脆弱性開示ポリシーを策定し、脆弱性の報告 (および修復) をタイムリーに行えるようにするための公開された連絡窓口を用意する必要があります。3) ソフトウェアを最新状態に維持 : ソフトウェアの更新は、タイムリーかつ実施が容易で、デバイスの機能を停止させないものである必要があります。

米国と英国が示した懸念とアプローチに基づき、IoT のセキュリティは引き続き政府の最優先事項となっています。また、国内外の標準化団体によって、IoT のセキュリティを確保するための標準、ガイドラインおよびベストプラクティスを策定する取り組みが進められています。[19] これには、国際標準化機構 (ISO) の IoT リファレンスアーキテクチャ、国際電気通信連合 (ITU) の IoT とスマートシティに関する研究グループなどが含まれます。[20]

IoT という観点では、お客様には、すでに使用され、より「従来型のネットワークサイバーセキュリティ」と考えられているもののうち、実績のある既存のプラクティスを利用する柔軟性が求められます。たとえば、脆弱性の特定、異常の検出、潜在的な

---

18 https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security を参照してください。

19 IoT セキュリティに関する現在の標準と取り組みの概要については、米国商務省国家電気通信情報庁 (NTIA) のカタログ (https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_17.pdf) を参照してください。

20 https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx を参照してください。

インシデントへの対応、および IoT デバイスの損傷または途絶からの復元を試みる場合、NIST のサイバーセキュリティフレームワーク (CSF) にマッピングされたサイバーセキュリティコントロールを使用できます。[21] このサイバーセキュリティの基本的な対策は世界的に認められており、業界や規模にかかわらず、あらゆる組織が利用するための推奨ベースラインとして政府や産業界から支持されています。NIST CSF を利用するメリットは、その評判だけでなく、物理的、サイバー的、および人間的な側面への影響を考慮しながらサイバーセキュリティを適用できる柔軟性にもあります。人間的側面に加えて、このフレームワークは、IT、産業制御システム、サイバー物理システム、または IoT のいずれに重点を置くかにかかわらず、テクノロジーに依存する組織に適用されます。

21 AWS のサービスを使用して NIST CSF と連携する方法の詳細については、このホワイトペーパーとお客様向けワークブック (https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf) を参照してください。

付録 3 – AWS IoT サービスとコンプライアンス

グローバルなハイパースケールクラウドサービスプロバイダとして、AWS は IoT サービスのセキュリティとお客様のデータの安全保護対策について厳格なリスクベースのアプローチを採用しています。AWS は、すべてのクラウドサービスに内部セキュリティプロセスを適用し、セキュリティとレジリエンスに影響を与える現在および将来のセキュリティ脅威から保護するために必要となる、経営面でのコントロール、技術的なコントロール、および運用面でのコントロールについて有効性を評価します。このような必須のセキュリティ保証プロセスによって、さまざまなコンプライアンスフレームワークへの認証が得られるだけでなく、サービスライフサイクルの開発および運用プロセスに存在するすべてのフェーズにセキュリティを組み込むという AWS のコミットメントも強化されます。AWS は、国際的に認められている主要な標準に認定された大規模な商用クラウドサービスを提供しています。認定を受けた標準には、ISO 27001、[22] PCI データセキュリティスタンダード (PCI DSS)、[23] Service Organization Control Reports (SOC)[24] をはじめとする、その他の国内外および業界の認定が含まれています。AWS は、特定の情報機関で使用される極秘情報を処理する環境をサポートするための厳しいセキュリティ要件にも対応しています。以上を総合すると、業種や規模にかかわらず、AWS Cloud サービスを利用しているお客様は、AWS という代理を通じてセキュリティに関するメリットを享受できます。その理由は、AWS がサービス全体に「高い基準のウォーターマーク」を適用しているからです。

お客様が特定のコンプライアンス要件を実証および遵守する必要があることについて、AWS は細心の注意を払っています。AWS では、お客様の要望に基づいてコンプライアンスプログラムに合わせたサービスを継続的に追加しています。対象となる IoT サービスは、AWS Web サイトにコンプライアンスプログラム別でリスト化されています。[25]

---

22 ISO 27001/27002 は世界的に広く採用されているセキュリティ標準であり、事業と顧客情報の管理について、刻々と変化する脅威のシナリオに適する定期的リスク査定に基づいた、体系的なアプローチの要件とベストプラクティスが規定されています。ISO 27018 は、クラウドにおける個人データの保護に焦点を当てた実施基準です。ISO 情報セキュリティ規格 27002 に基づいており、パブリッククラウドの個人識別情報 (PII) に適用される ISO 27002 統制の実装ガイダンスを提供しています。また、既存の ISO 27002 コントロールセットでは対応していないパブリッククラウド PII 保護要件に対応するための追加のコントロールセット、および関連ガイダンスも提供しています。

23 PCI データセキュリティスタンダード (PCI DSS) は機密情報に関するセキュリティ基準であり、American Express、Discover Financial Services、JCB International、MasterCard Worldwide、Visa Inc. が設立した PCI Security Standards Council (https://www.pcisecuritystandards.org) によって管理されています。PCI DSS は、加盟店、プロセッサ (決済処理代行事業者)、カード会社、サービスプロバイダを含め、カード所有者データ (CHD) や機密認証データ (SAD) を保存、処理、転送するすべての団体に適用されます。

24 Service Organization Controls レポート (SOC 1、2、3) は、米国および国際的な会計監査機関の監査における幅広い要件を満たすために作成されています。このレポートの監査は、International Standards for Assurance Engagements 第 3402 号 (ISAE 3402) およびアメリカ公認会計士協会 (AICPA) AT 801 (旧称 SSAE 16) に従って実施されます。

25 https://aws.amazon.com/compliance/services-in-scope を参照してください。