CSA IoT セキュリティコントロール フレームワーク　利用ガイド

日本語版：一般社団法人　日本クラウドセキュリティアライアンス

謝辞

イニシアティブリーダー

Brian Russell
Michael Roza

主な協力者

Hillary Baron
Daniele Catteddu
Luciano Ferrari
Aaron Guzman
Ankur Gargi
Sabri Khemissa
Douglas Mcdorman
Todd Nelson
Eric Palmer
J.R. Santos
Theodoros Stergiou
Srinivas Tatipamula
John Yeoh

CSA Internet of Things (IoT) Working Group について:
コネクテッドデバイスやサイバーフィジカルシステムは、企業環境で一般的になっています。クラウド環境がこれらのテクノロジーを網羅するように拡大するにつれて、接続された世界はデータを管理、調整、およびプロビジョニングするためにデバイスに依存します。 CSA IoT ワーキンググループは、これらのコネクテッドシステムを保護するためのフレームワーク、プロセス、そして最もよく知られている方法を開発しています。 IoT ワーキンググループは、データのプライバシー、フォグコンピューティング、スマートシティーなどを含むトピックを扱います。詳しくは、このリンクを参照してください。.

日本語版提供に際しての告知及び注意事項

本書「CSA IoT セキュリティコントロールフレームワーク　利用ガイド」は、Cloud Security Alliance (CSA)が公開している「Guide to the CSA Internet of Things (IoT) Security Controls Framework」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。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。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2019 年 11 月 28 日	日本語版 1.0	初版発行

日本語版作成に際しての謝辞

この日本語訳は、CSA ジャパン IoT ワーキンググループに参加するメンバーにより行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。
（氏名あいうえお順・敬称略）

有本　真由
甲斐　　賢（株式会社日立製作所）
勝見　　勉
二木　正明

CSA ジャパン IoT WG について

CSA ジャパン IoT ワーキンググループは、上記グロー-バルワーキンググループとの連携のもとで、独自の知見をフィードバックすると同時に、各種文書の日本語化と普及活動を行っています。独自に様々なリサーチ活動を実施し、日本の状況に応じたアウトプットを提供しています。詳細については、こちら をご覧さい。

目次

はじめに

このクラウドセキュリティアライアンス（CSA）Internet of Things（IoT）セキュリティコントロールガイドは、関連 CSA IoT セキュリティコントロールフレームワークスプレッドシートの使用方法について説明しています。 このガイドでは、フレームワークを使用して組織の IoT システムを評価および実装する方法について説明します。 欧州連合情報セキュリティ庁（ENISA）は、IoT システムを「相互に接続されたセンサーとアクチュエーターのサイバーフィジカルエコシステムであり、これによりインテリジェントな意思決定が可能になるもの」と定義しています。

IoT セキュリティコントロールフレームワークは、複数の種類の接続デバイス、クラウドサービス、およびネットワークテクノロジを組み込んだエンタープライズ IoT システムに関連しています。 このフレームワークは、影響度の限られた「価値の低い」データのみを処理するシステムから、重要なサービスをサポートする非常に機密性の高いシステムまで、多くの IoT 領域にわたって有用です。 システムの分類は、格納および処理されているデータの価値と、さまざまな種類の物理的なセキュリティ上の脅威による潜在的な影響に基づいて、システムの所有者が割り当てます。

このフレームワークは、ユーザーが適切なセキュリティ管理策を特定し、それらを IoT システム内の特定の構成要素に割り当てるのに役立ちます。それらは以下を含みますが、それに限定はされません。

・単純なセンサー
・単純なアクチュエーター（駆動装置）
・エッジデバイス
・フォグ・コンピューティング
・モバイルデバイス・アプリケーション
・オンプレミスの中継デバイス
・クラウドゲートウエイ
・クラウドアプリケーション・サービス

対象とする読者

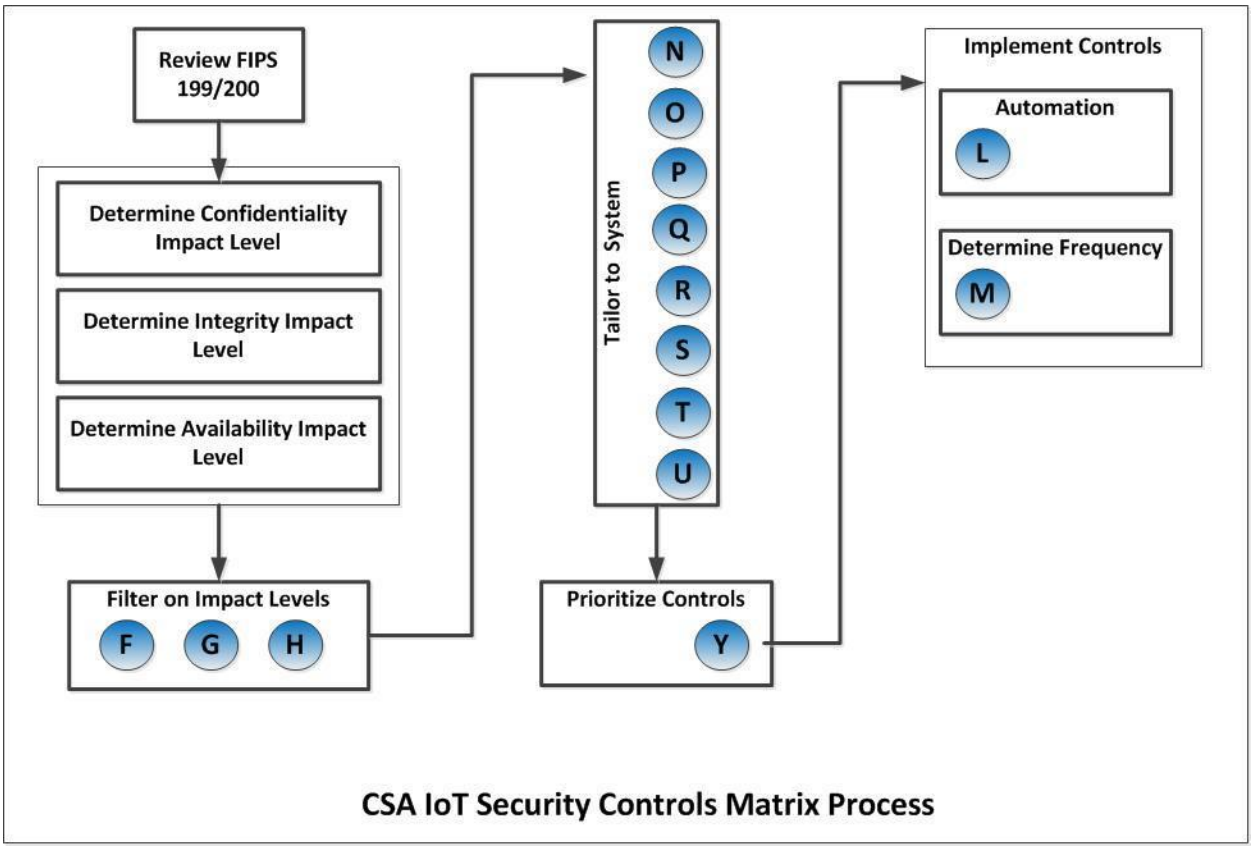
IoT セキュリティコントロールフレームワークは、安全な IoT システムを作成することを任務とする設計者と、開発者、および、その他の IoT システムの評価者のためのリソースです。 設計者および開発者はこのツールを使用して、開発ライフサイクルの進行中に実装のセキュリティを継続的に評価できます。 このツールは、業界固有のベストプラクティスを確実に満たすために、IoT システムの全体的な評価を提供します。

このバージョン（バージョン１）の内容

IoT セキュリティコントロールフレームワークのバージョン 1 では、さまざまな脅威環境で動作する IoT システムに関連する多くのリスクを軽減するために必要な基本レベルのセキュリティコントロールを紹介しています。 このフレームワークの今後のバージョンに対する CSA の計画には、適用可能なテストガイダンス、および業界のベストプラクティスを他の主要な IoT セキュリティ組織と協調させることが含まれています。

CSA IoT セキュリティコントロールフレームワークの使い方

下の図 1 は CSA IoT セキュリティコントロールフレームワークのユーザーが独自の環境のセキュリティコントロールを評価して実装する際に従うべきフローを示しています。 この図の丸で囲まれた文字は、フレームワーク（スプレッドシート）の列に対応しています。



なお、日本語訳版では、英語原文も残しており、列 A にフィルタ用カラムを設け、日本語と英語もしくはその両方の表示を選択できるようにしています。このため、オリジナルに対して、各列が右に一列ずれていますのでご注意ください。

セキュリティコントロールの目的（列 B,C,D,E）

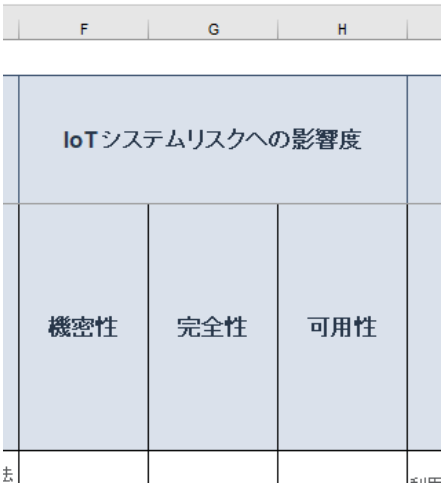
コントロール種別（ドメイン：列 B）：列 E（コントロールの内容）で詳しく書かれている個々のセキュリティコントロール方法を論理的にグルーピングしたもの。対応するコントロールの内容は斜体で表示されています。

コントロール ID（列 C)：特定のセキュリティコントロールに対する識別子で、関連付けられた英字略称と番号は、このフレームワークの他の場所から、それが示すコントロールを参照するために使われます。.

CCM ID（列 D）：このフレームワーク内のセキュリティコントロールは CSA クラウドコントロールマトリクス（CCM）から派生するか、関連している場合に、この列によって、ひとつもしくは複数の CCM のコントロール識別子と対応づけられます。関連付けられたコントロールは、各フレームワークにおけるコントロール内容の一部または全部をカバーします。

コントロールの内容（列 E）：内容は、IoT システムの特定のリスク領域に対処するための緩和策または対策として書かれています。 使いやすさを考え、各コントロールは固有の IoT 環境に対処できるよう、単純化されたアクションに分けられています。

IoT システムリスクの影響度（列 F,G,H）



列 F から列 H までは、ユーザー独自の環境に合わせてセキュリティ管理策を最初にカスタマイズすることを可能にします。 独自のセキュリティ管理をカスタマイズするプロセスを開始する前に、米国商務省の 2 つの出版物「連邦情報情報システムのセキュリティ分類基準」（FIPS 199）と「連邦情報情報システムの最低セキュリティ要件」を確認してください。 （ＦＩＰＳ２００）２。 FIPS 199[1]および 200[2]では、次の 3 つの要素でリスク影響レベルを低、中、高に分類しています。:

機密性（列 F）：個人のプライバシー情報や固有情報など、IoT システム内の一部のデータでは、適切に機密を保持するためにさまざまなセキュリティ管理によるアクセス制限が必要です。 IoT システムの機密性リスクの要素を評価するには、システムのデータが公開された場合や攻撃者によって侵害された場合に、潜在的な影響がどの程度（低、中、高）になるかを評価する必要があります。
完全性（列 G）：データの完全性を保護するために、企業はデータの不適切な変更または破壊から保護し、情報の信頼性を保証する必要があります。 IoT システムの整合性リスクのさまざまな要素を評価するには、システムを流れるデータが破壊されたり不適切に変更されたりした場合の影響を評価します（低、中、高）。

[1] FIPS 199：「連邦情報および情報システムのセキュリティ分類のための標準」、米国商務省コンピュータセキュリティ部門の連邦情報処理標準文書。 https：// nvlpubs.nist.gov / nistpubs / FIPS / NIST.FIPS.199.pdf
[2] FIPS 200：「連邦情報および情報システムのための最低限のセキュリティ要件」、連邦情報処理標準文書、米国商務省コンピュータセキュリティ部門。 2006 年 3 月。https：// nvl-pubs.nist.gov / nistpubs / FIPS / NIST.FIPS.200.pdf

可用性（列 H）：システム内の情報がタイムリーかつ信頼できる方法でアクセス可能であり続ける必要がある度合を評価するには、システムが一定期間稼働できなくなった場合の潜在的なリスクを評価する必要があります。.

システムのデータの機密性、完全性、および可用性に関する特定のリスクが、低、中、高のどれであるかを評価するには、FIPS 199「セキュリティの目的に対する潜在的影響の定義」の 6 ページの表 1 を参照してください。

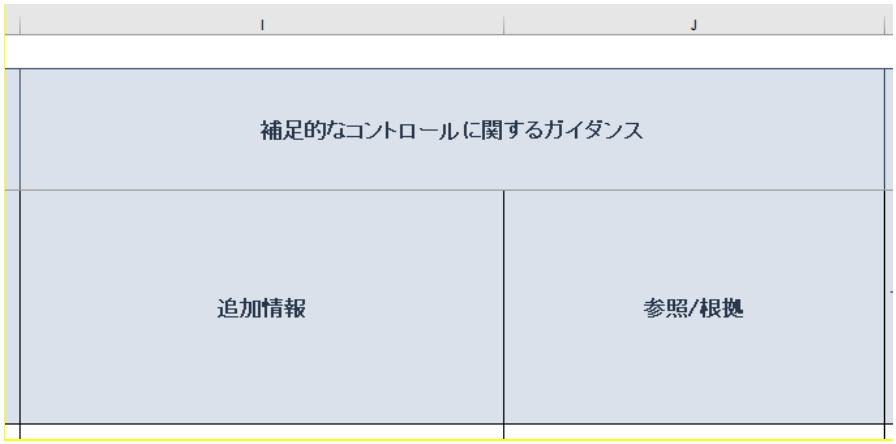
これらのリスク影響レベルを決定したら、IoT セキュリティコントロールフレームワークを使用して、固有の環境に実装するために必要なすべてのセキュリティコントロールを識別できます。

影響レベルが高の場合、低、中、高リスクレベルを含むすべてのセキュリティコントロールを適用する必要があることに注意してください。影響レベルが中程度の場合、中程度および低リスクレベルのすべてのコントロールを適用する必要があります。

以下は、3 つの影響評価と必要な対応するコントロールの例です。

セキュリティリスクのタイプ（例）	リスクの影響レベル（例）	必要なセキュリティコントロール
機密性	高	高、中、低
完全性	中	中、低
可用性	低	低のみ

コントロールガイダンスの補足（I, J 列）



追加の指示（列 I）：IoT セキュリティコントロールフレームワークの個々のセキュリティプロトコルを評価または実装するときは、特別な要件、用語の説明、役立つ操作のヒントなどを詳述するこの補足情報を必ず見てください。.

参考文献/根拠（列 J）：管理仕様を完全に理解するために必要な、政府出版物、規制情報、およびその他の参考文献などの専門的な情報源については、このセクションを参照してください。

実装ガイダンス（K,L,M 列）

セキュリティ計画の自社への実装に際しては、「実装ガイダンスのフレームワーク」のセクションを使って、自社に固有の環境に必要な管理のタイプ（コラム K）、 自社がそれらを実行することができる方法（コラム L）、 そして各セキュリティコントロール手段の必要な実施頻度（列 M）を決定してください。

セキュリティコントロールのタイプ（K 列）

IoT フレームワークのセキュリティ管理策は、いつ、どこで、どのように対策がセキュリティを強化するために機能するかに基づいて、3 つのタイプに分類されます。

予防型コントロールは、何かが起きるのを防ぎます。たとえば、施錠されたドアを用いたりより高いレベルの生体認証によって、部屋への物理的なアクセスを制限します。

検知型コントロールは、インシデントを識別し、特性分けします。 例としては、実地検数後の在庫の食い違いの調査 、ビデオ録画、 不法侵入を検出するためのモーションセンサーの使用などがあります。

是正型コントロールは、消火器で火災により起こりうる被害を軽減したり、プライマリデータセンターが停止した場合の複製データセンターの可用性など、セキュリティインシデントによって引き起こされる損害を軽減します。

コントロールの実装（L 列）

セキュリティコントロールは、自動化のレベルに応じて 3 つの方法で実装されます。

手動型コントロールは人間によって行われます。 たとえば、リスク管理プロセスのレビューでは、誰かがプロセスを評価して、それがポリシーに従って実行されたことを確認します。

自動型コントロールは、人手を介さずにシステムによって実行されます。 たとえば、ユーザーアクセスチェックでは、ユーザーはユーザー名とパスワードでログインします。 システムはアクセスを許可する前に組み合わせを検証します。

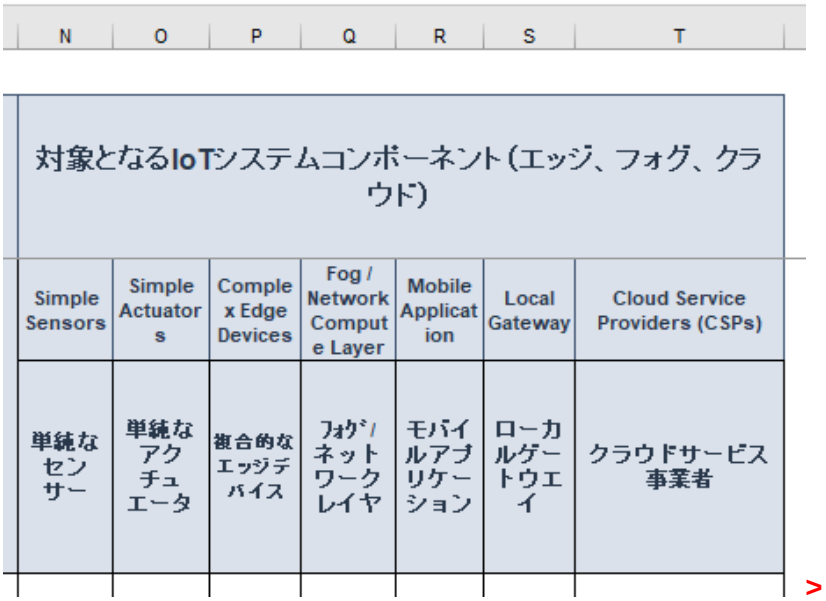
半自動型コントロールは自動化と手動の対処を組み合わせたものです。 たとえば、実地棚卸では、品目がカウントされ、結果がシステムが生成したリストと比較されます。 相違があれば調査によって是正しますが、その際、紙ベースと電子的記録の両方を利用します。

コントロールの実施頻度（M 列）

個々の企業のニーズに応じて、セキュリティコントロールの実行には異なる頻度が必要です。組織によっては、内部のリスク対策の優先度や法令順守の要求に応じて、より頻繁な管理を必要とします。 さまざまな状況に対応して、次の頻度が推奨されます。

- 毎年
- 四半期ごと
- 毎月
- 毎週
- 毎日
- イベント毎：制御は不規則に実行されます。 例：ソフトウェアのアップデート
- 常時：1 日に何回もコントロールが実行されます。 例：ユーザーアクセス

エッジ、フォグ、クラウドにおける IoT システムのコンポーネント（N～T 列）



N	O	P	Q	R	S	T
対象となるIoTシステムコンポーネント(エッジ、フォグ、クラウド)						
Simple Sensors	Simple Actuators	Complex Edge Devices	Fog / Network Compute Layer	Mobile Application	Local Gateway	Cloud Service Providers (CSPs)
単純なセンサー	単純なアクチュエータ	複合的なエッジデバイス	フォグ/ネットワークレイヤ	モバイルアプリケーション	ローカルゲートウェイ	クラウドサービス事業者

>

列 N から列 T までは、要件が IoT システムのコンポーネントに適用されるかどうかを識別します。 たとえば、一部の要件はエッジデバイスにのみ適用され、その他の要件はゲートウェイまたはクラウドサービスにのみ適用されます。 IoT セキュリティコントロールフレームワークは、特定の IoT システム実装に合わせてセキュリティ要件を調整できるように設計されています。 そして、エッジ、ネットワーク、クラウドなどを含む IoT システム内の共通コンポーネントが、対応する要件とともに識別されています。.

エッジ（N 列、O 列、P 列）

エッジでは、データはさまざまなセンサーを介して物理的な世界から入り、さまざまな形式の出力とアクチュエーターを介して物理的状態を変更するためのアクションが取られます。パフォーマンスを発揮するエッジデバイス分析を行い、知識を生成し、中央データセンターと接続システム間で行われる通信に必要な帯域幅を最小限に抑えます。たとえば、自動運転は、クラウドまたはデータセンターに接続しますが、安全性を確保するためにエッジノードのサイトでの分析と処理も必要です。エッジで分析を実行することには、近接したデバイス間、または有用な関連テクノロジーとのデバイス間のコラボレーションも含まれます。エッジコンピューティングは、上記のような製造プロセスも可能にします。たとえば、ダウンストリームデバイスにアップストリームプロセスの遅延を通知し、問題が解決している間、エネルギーを節約することができます。

単純なセンサー（N 列）：エッジデバイスは、処理、ストレージ、およびネットワーク機能が非常に限られています。これらの装置の例示的な特性は、電池電力、節電のためのスリープモード、圧力や温度などの単一の情報を取得して送信するように設計されたマイクロコントローラがあります。これらのセンサーに適用されるセキュリティ制御は、ハードウェア機能に制限されています。ただし、ゲートウェイやクラウドなど、他のレベルでこれらのセンサーにセキュリティを追加することもできます。

単純なアクチュエーター（駆動装置）（O 列）：これらのエッジデバイスは、処理、保管、ネットワーク機能にも制限がありますが、ポンプ操作のような物理的機能を実行します。 単純なセンサーと同様に、一般的に堅牢なセキュリティ管理機能はありません。

複合エッジデバイス（P 列）：ソフトウェアまたはハードウェアの暗号化セキュリティモジュールを組み込むなど、高度なセキュリティ要件を満たすことができるデバイス。

ネットワーク（Q 列、R 列、S 列）

ネットワークでは、フォグコンピューティングノード（Q 列）が、分析、ノード管理、およびポリシー管理を実行します。ローカルの IoT ゲートウェイ（R 列）などのインフラストラクチャ機器は、ワイヤレスセンサーネットワークなどの様々な IoT デバイスからのデータを集約します。モバイルアプリケーション（S 列）は、リモート管理を含む様々な IoT サービスをサポートするために、IoT デバイスおよび関連するクラウドサービスと連携します。

フォグ／ネットワークコンピューティングレイヤ（Q 列）：以下のように、米国商務省標準技術院（NIST）によって定義される通りです。

「フォグコンピューティングは、スケーラブルなコンピューティングリソースの共有連続体へのユビキタスアクセスを可能にするための階層化モデルです。このモデルは、レイテンシを考慮した分散型アプリケーションおよびサービスの展開を容易にし、スマートエンドデバイスと集中型（クラウド）サービスとの間に存在する（物理的または仮想上の）フォグノードで構成されています。フォグノードは、コンテキストに配慮し、共通のデータ管理および通信システムをサポートします。フォグノードは、垂直方向（分離をサポートするため）、水平方向（フェデレーションをサポートするため）、またはスマートエンドデバイスまでのフォグノードのレイテンシを基準にして、クラスタ化することができます。フォグコンピューティングは、サポートされているアプリケーションとの間の要求/応答時間を最小限に抑え、エンドデバイスにローカルコンピューティングリソース、および必要に応じて集中サービスへのネットワーク接続性を提供します。」

ノードは、フォグレイヤーでは、IoT デバイスからリアルタイムでフィードを受信します。 フォグノードは、ミリ秒の応答時間で、リアルタイム制御と分析のために IoT 対応アプリケーションを実行します。ノードは、多くの場合 1〜2 時間の間、一時的なストレージを提供し、その後、定期的にデータの概要をクラウドに送信します。

モバイルアプリケーション（R 列）：IoT デバイスまたはサービスとペアになっている、またはそれらと対話するアプリケーションまたはユーザーインターフェイス。

ローカルゲートウェイ（S 列）：ゲートウェイは、ローカルアプリケーションレイヤーの MQTT ブローカーや、ローカルワイヤレスセンサーネットワーク（WSN）通信を集約する通信ゲートウェイなど、エッジデバイスへの接続器またはコントローラです。

クラウド（T 列）

クラウドサービスプロバイダー、または CSP（T 列）：エッジデバイスに接続するクラウドアプリケーション、サービス、およびゲートウェイは、機械学習、音声認識、イベント処理、データ分析、メッセージング、通知、データベース管理、およびレジストリやロギングなどのサイバーセキュリティサービスなど、様々な IoT 機能をサポートします。クラウド内のゲートウェイはエッジデバイスに接続します。これらのゲートウェイは、アプリケーションレイヤゲートウェイ（MQTT ブローカーなど）または CSP の前面にある通信ゲートウェイです。

参考文献

Fujitsu Develops Data Processing Architecture "Dracena," Can Reconfigure Content within IoT Data Processing Stream; Fujitsu Laboratories Ltd., Kawasaki, Japan, March 7, 2018. http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0307-02.html

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), Draft NISTIR 8200; National Institute of Standards and Technology; February 2018.https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

“Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” European Union Agency for Network and Information Security (ENISA); November 20, 2017.
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

“Internet of Things--Reference Architecture,” ISO/IEC JTC 1/SC 41; August 2018.https://www.iso.org/standard/65695.html

“Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff,” U.S. Food and Drug Administration (FDA), Section IV; January 22, 2016.
https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

“Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices: Guidance for Industry and Food and Drug Administration Staff,” U.S Food and Drug Administration (FDA); January 26, 2016.
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf

“THE FDA’S ROLE IN MEDICAL DEVICE CYBERSECURITY: Dispelling Myths and Understanding Facts,” U.S. Food and Drug Administration (FDA) Fact Sheet.
https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf

“Trusted and Secure Wireless Sensor Network Designs and Deployments,” by Ignacio Bravo, Esther Palomar, Alfredo Gardel and José Luis Lázaro; *Sensors: an Open Access Journal*, August 4, 2017.
http://www.mdpi.com/1424-8220/17/8/1787/pdf

“Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 1; April 2014.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS),” Internet Engineering Task Force (IETF) RFC 7525; May 2015. https://tools.ietf.org/html/rfc7525

“Internet of Things Security Best Practices,” Microsoft Azure. https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices

“Internet of Things (IoT) Trust Concerns,” by Jeffrey Voas, Richard Kuhn, Phillip Laplante, and Sophia Applebaum; NISTIR 8222; September 2018. https://csrc.nist.gov/publications/detail/nistir/8222/draft

“Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths,” by Elaine Barker and Allen Roginsky; NIST SP 800-131A Revision 1; November 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

“Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” by Kaitlin Boeckl, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina Megas, Ellen Nadeau, Ben Piccarreta, Danna Gabel O'Rourke, and Karen Scarfone; NISTIR 8228 (DRAFT), September 2018. https://csrc.nist.gov/publications/detail/nistir/8228/draft

“Fog Computing Conceptual Model, Recommendations of the National Institute of Standards and Technology,” by Michaela Iorga, Larry Feldman, Robert Barton, Michael J. Martin, Nedim Goren, and Charif Mahmoudi; NIST SP 500-325, March 14, 2018. https://www.nist.gov/publications/fog-computing-conceptual-model

“Fog Computing Conceptual Model: Recommendations of the National Institute of Standards and Technology,” National Institute of Standards and Technology (NIST) Special Publication 500-325. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf