CSA IoT Controls Matrix v3 ガイド

cloud security alliance®

Cloud Security Alliance Internet of Thingsの研究の常設・公式拠点は、
https://cloudsecurityalliance.org/working-groups/internet-of-things/。

Acknowledgments

The CSA IoT Controls Matrix is updated and released at least annually. The following volunteers have generously contributed to the matrix over its lifetime.

Initiative Leads

Aaron Guzman
Michael Roza
Brian Russell

Contributors v3

Raj Sachdev
Gerry Gajeton

Contributors Prior to v3

Luciano Ferrari
Ankur Gargi
Sabri Khemissa
Douglas Mcdorman
Todd Nelson
Eric Palmer Theodoros
Stergipou Srinivas
Tatipamula

Reviewers

Cheryl Flannery
Ashish Vashishtha

CSA

Hillary Baron
Claire Lehnert
J.R. Santos John
Yeoh

日本語版提供に際しての告知及び注意事項

本書「CSA IoT Controls Matrix v3ガイド」は、Cloud Security Alliance (CSA)が公開している「Guide to the CSA IoT Controls Matrix v3」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
2022年06月28日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3. 本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. 原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「CSA IoT Controls Matrix v3ガイド」は、CSAジャパン会員の有志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を記します。（氏名あいうえお順・敬称略）

白石　敬典
諸角　昌宏
山崎　英人
山下　亮一

目次

はじめに 8
マトリックスの調整 8
業界プロファイル 9
ゴール 9
対象とする利用者 9
バージョンについて 9
IoTセキュリティコントロール フレームワークの使い方 10
セキュリティコントロールの目的（A,B,C,D,E,F列） 11
IoTシステムリスクの影響度（G、H、I列） 13
補足的なコントロールガイダンス（J、K欄） 14
実施ガイダンス（L、M、N列） 14
セキュリティコントロールのタイプ（L列） 15
コントロール実施ガイダンス（M列） 15
コントロールの見直し期間（N列） 15
デバイス、ネットワーク、ゲートウェイ、クラウドサービス（O、P、Q、R） 16
その他のリソース 18

はじめに

モノのインターネット（IoT）市場は、業界全体において接続性（connectivity）と自律性（autonomy）の面での新たな進化により拡大を続けています。IoTで生成されたデータや機能への依存により、これらの新しいテクノロジーを採用する組織は、アクセス可能で、安全で、レジリエンスのある配備を計画する必要があります。コネクテッドテクノロジーの急速な進化と新たな脅威の絶え間ない発生を考えると、その実現は容易ではありません。安全なIoT環境を構築するには、固有のリスクに対処し、適切なリスク緩和策を実装することができるセキュリティエンジニアリングが必要です。クラウドセキュリティアライアンス（CSA）のIoTセキュリティコントロールフレームワークは、組織がそのIoTアーキテクチャに必要なセキュリティコントロールをよりよく理解し、実装するための起点となります。このガイドでは、企業組織がこのフレームワークを使用して、IoTシステムを安全に評価および実装する方法について説明します。

マトリックスの調整

IoTセキュリティコントロールフレームワークは、多様なコネクテッドデバイス、関連するクラウドサービス、ネットワーク技術、およびアプリケーション・ソフトウェアを展開するエンタープライズIoTシステムのために提供するものです。このフレームワークは、インパクトが生じる可能性が低い「低価値」の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機密性の高いシステムまで、多くのIoTドメインで利用可能です。システム所有者は、保存・処理されるデータの価値と、様々な物理的セキュリティ脅威の潜在的影響に基づいてコンポーネントを分類します。

このフレームワークは、ユーザーが適切なセキュリティコントロールを特定し、それを以下のような特定のアーキテクチャコンポーネントに割り当てるのに役立ちます。

- デバイス
- ネットワーク
- ゲートウェイ
- クラウドサービス

アーキテクチャの各レイヤーに割り当てられたコントロールは、ベストケースのセキュリティポスチャを表しています。場合によっては、アーキテクチャコンポーネントが、このフレームワークで特に推奨される管理策を実施できないことがあります。このような場合、システムセキュリティアーキテクトはそれらの欠点を特定し、代替手段を用いて残留リスクを緩和するための計画を策定する必要があります。

このフレームワークは、特定のサイバーセキュリティアーキテクチャの目標に合わせて調整することができます。例えば、ゼロトラストに関する具体的なコントロールは含まれていませんが、セキュリティエンジニアは、フレームワークを使用して、ゼロトラストアーキテクチャ（ZTA）を実現するためのコントロールを特定することが可能です。マイクロセグメンテーション（SNT-04）、特権的サービス操作の制限（IAM-04）、ネットワークへのブートストラッププロセス（IAM-07）、デバイス認証を前提としたSDP（Software Defined Perimeter）構成（SNT-02）といったコントロールは、デバイスベースのZTA構築の起点として使用することができます。

業界プロファイル

本ガイドのバージョン3では、業界プロファイルが追加されました。これらのプロファイルは、医療機器、車両、一般的な自律システムなど、業界特有のIoTデバイスを保護するための出発点となります。バージョン4では、車両や一般的な自律システムの制御、およびICS/IIoTの制御が追加される予定です。

ゴール

IoTセキュリティコントロールフレームワークは、開発ライフサイクルを通じたセキュリティ実装をガイド・評価し、業界固有のベストプラクティスを満たしているかどうかを確認するためのツールです。

対象とする利用者

IoTセキュリティコントロールフレームワークは、セキュアなIoTエコシステム設計を担当するシステムアーキテクト、開発者、セキュリティエンジニア向けのリソースです。監査人や侵入テスターなどのIoTシステム評価者は、このフレームワークを活用してコントロールとその実装されたもの（状態）を検証することができます。

バージョンについて

バージョン1では、様々な脅威環境で動作するIoTシステムが直面する多くのリスクを軽減するために必要な160の基本レベルのセキュリティコントロールが紹介されています。

バージョン2では、バージョン1のフレームワークを進化させ、コントロールを新しいドメインセットに分類し、IoTアーキテクチャ内のコンポーネントへのコントロール割り当てを最小化し、セキュリティコントロールを155に削減しました。

バージョン3では、**バージョン２**のフレームワークを進化させ、コントロールの数を199に増やし、新しいインシデント管理ドメインを追加し、技術的な明確性と参照性を向上させています。

バージョン4では、以下のような改良が加えられる可能性があります：

- サプライチェーンドメイン
- 車両制御、汎用自律システム制御、ICS/IIoT制御
- IoTフレームワーク 責任共有マトリクス
- 安全性固有のコントロール
- 侵害指標（IoC：Indicator of Compromise）
- ENISA（欧州ネットワーク情報セキュリティ機関）IoTセキュリティのためのガイドライン（Guidelines for Securing the Internet of Things）とのマッピング
- NIST（米国国立標準技術研究所）サイバーセキュリティフレームワーク（CSF）及びSP800-53とのマッピング
- NIST Informative Reference Classification Application

IoTセキュリティコントロール フレームワークの使い方

右の図1は、CSA IoTセキュリティコントロールフレームワークの利用者が、独自環境におけるセキュリティコントロールを評価・実装する際に従うべきフローを示しています。図中の括弧内の文字は、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。

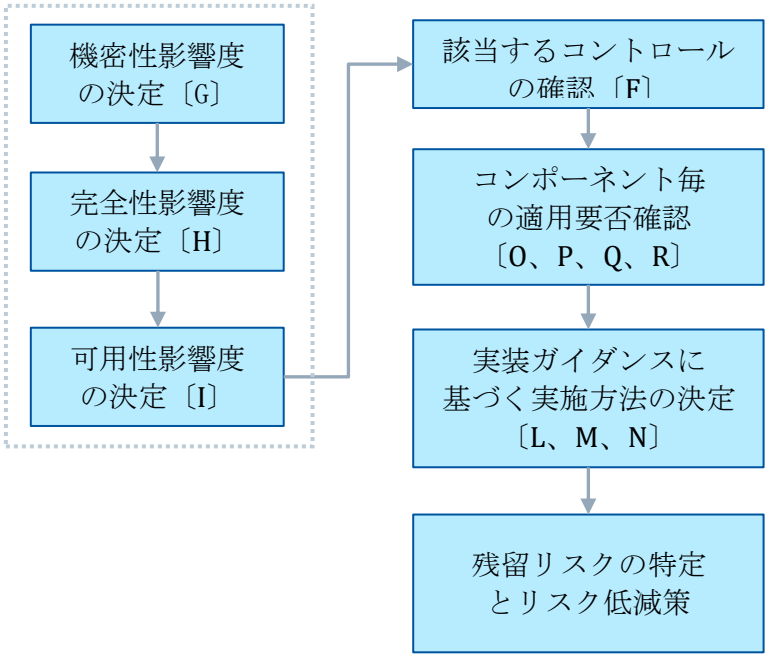


図1 - コントロールアセスメント

日本語版注記）
S列（Language）に、それぞれの行の記述が英語（EN）あるいは日本語（JP）であるかどうかを記述しています。S列の値でフィルタリングすることで、英語のみの表記あるいは日本語のみの表記にすることができます。

評価は、システムアーキテクチャのセキュリティとデータへの影響度を理解することから始まります。これらは、連邦情報処理標準(FIPS)199などの標準プロセスに基づいて特徴付けられます。システムの機密性、完全性、可用性について影響度の判定が行われると、フレームワークにフィルタをかけて、その影響度に該当するコントロールのみを表示することができます。

フレームワークをフィルタリングした結果の各コントロールをF列で確認し、J列で追加のガイダンスを確認します。O, P, Q, R の各列には、様々なコンポーネント配置によりコントロールを適用する必要があるかどうかが示されています。これらの列では、デバイス、デバイスをホストするネットワーク、ゲートウェイ、クラウドサービスのいずれに適用するかの観点でコントロールをフィルタリングすることができます。

また、L, M, Nの列には、コントロールの種類、コントロールを手動、自動、またはその両方の組み合わせのいずれの方法を適用すべきかどうか、コントロールを実行する頻度が記載されています。

この最初のプロセスの後、フレームワークは、IoTシステムアーキテクチャに応じたセキュリティ基準の理想的なバージョンに関する洞察を提供します。IoT アーキテクチャ内の一部のコンポーネントは、コントロールのサブセットを満たすことができない場合があります。このような場合、セキュリティアーキテクトは残留リスクを理解し、そのリスクを軽減するための補完的コントールを特定しなければなりません。

セキュリティコントロールの目的（A, B, C, D, E, F列）

A	B	C	D	E	F
			For more details about the framework, download the "Guide to the CSA IoT Controls Matrix" at: <link>		
Control Domain	Control Domain	Control Sub-Domain	Control ID	CCM v4 Domain	Control

コントロールドメイン（A列）：F列（Control）に詳細に詳述されている個々のセキュリティコントロールを、論理的にグループ分けしたもの（下表参照）。" Control Domain "のカテゴリの下に、対応する各コントロールの仕様の名称を斜体で記載しています。

コントロールドメイン(B列)：ドメインはフィルタリングのために分類されています。

コントロールサブドメイン(C列)：サブドメインは、フィルタリングのための詳細な情報を提供しています。

#	制御領域	Abbr.	コントロールサブドメイン
1	資産管理	ASM	命名規則、資産目録、資産監視
2	構成管理	CON	設定ファイル、ファームウェアの更新、構成制御。 EOL（End of Lile）管理計画
3	クラウドサービス	CLS	クラウドIAM、クラウドデータセキュリティ、クラウドインフラセキュリティ、クラウド監視、クラウドAPIセキュリティ
4	セキュアなデータ	DAT	データ分類と分類方法、データクレンジング、保存されている暗号化されたデータ
5	ガバナンス	GVN	ガバナンスフレームワーク、規制および法的要件、コンプライアンス管理、プライバシー、事業継続性、安全性
6	アイデンティティ・アクセス管理	IAM	パスワード管理、認証、認可、アクセス制御、証明書管理、鍵管理、トラストアンカー管理、ブートストラップ、アカウント監査
7	インシデント管理	IMT	インシデント計画、インシデント対応、コラボレーション、修復、フォレンジック、自動化
8	IoTデバイスのセキュリティ	IOT	認定デバイス、セキュアなプラットフォーム、セキュアな構成
9	法的問題	LGL	法的評価、法的な実施計画、法的目的のための文書化措置、利用規約とプライバシーポリシー、契約、免責事項、開示、通知、権利放棄、責任、データ移転

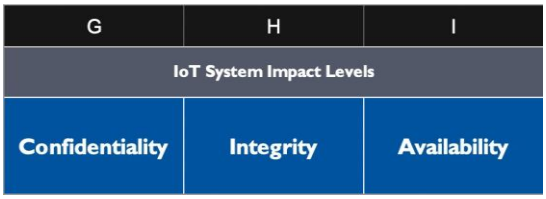
10	監視とロギング	MON	脅威インテリジェンス、脅威ハンティング、自動化されたマルウェア、ログ管理、分析、攻撃検知、 無線周波数（RF）モニタリング、ネットワーク可視化
11	運用の可用性	OPA	メンテナンス、フェイルオーバー、DDoS対策、サービスレベルアグリーメント
12	物理的セキュリティ	PHY	物理的アクセス制御
13	ポリシー	POL	ポリシー定義、買収に係るセキュリティポリシー、安全な処分
14	リスク管理	RSM	リスク管理戦略、リスク管理の実行、信頼性の制限
15	セキュアなアプリケーション	SAP	モバイルアプリケーション、ICS/IIoT、自律システム、自動車、医療機器
16	セキュアなシステム開発ライフサイクル	SDV	プロセスセキュリティ、サプライチェーン／買収、セキュアな開慣行
17	セキュアなネットワークス	SNT	セキュアメッセージング、セキュアディスカバリー、自動化、暗号化、セグメント化／VLAN、ネットワークアクセス制御、SDP（Software-Defined Networking）、ハードニング、 Single Packet Authentication 、セキュアメッセージング、ホワイトリスト化
18	セキュアなワイヤレス通信	SWS	ワイヤレス通信アーキテクチャ、Bluetoothセキュリティ、 近距離無線通信（NFC）セキュリティ、Zigbeeセキュリティ、ZWaveセキュリティ、LoRaWANセキュリティ、セルラーセキュリティ、衛星セキュリティ、WiFiセキュリティ、ワイヤレス通信アベイラビリティシステム
19	トレーニング	TRN	管理者向けトレーニング、ユーザー向けトレーニング
20	脆弱性管理	VLN	責任ある開示プログラム、脆弱性スキャン、アップデート、パッチ適用
21	セキュリティテスト	SET	評価の範囲と計画、ペネトレーションテスト、レッドチーム、サードパーティの評価、バグバウンティ、IoTアプリケーションとサービス（社内開発）。

コントロールID（D列）：コントロールIDは、特定のセキュリティコントロールに対する正式な識別子です。ID（例："RSM-01"）は、フ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 ドメイン（E 列）：フレームワークのセキュリティコントロールは、この列で CSA Cloud Controls Matrix （CCM）のドメインに関連付けられ、マッピングされています。IoT セキュリティコントロールがCCMコントロールに派生またはリンクされる場合、1 つまたは複数のエントリが識別されます。関連するコントロールは、各フレームワークのコントロール仕様の一部または全部をカバーします。

コントロールの記述（F列）：IoT システムの特定のリスク領域に対応する緩和策または対策として、仕様が記述されています。使い勝手を考慮し、各コントロールは固有のIoT環境に対応するための簡略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（G, H, I列）



G列からI列：この情報により、ユーザー独自の環境に合わせた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。個々のセキュリティ管理策をカスタマイズするプロセスを開始する前に、ユーザーは米国商務省の2つの出版物を確認する必要があります。「連邦政府の情報および情報システムに対するセキュリティ分類規格」（*FIPS 199*）[1]および「連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項」（*FIPS 200*）[2]です。これらの出版物は、機密性、完全性、可用性の3つの分野で、リスクインパクトのレベルを「低」、「中」、「高」に分類しています。

機密性（G列）：IoTシステムのデータの中には、個人のプライバシーや固有情報など、適切な機密性を保つために、様々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ためには、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（H列）：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や破壊を防ぎ、情報の信頼性を確保する必要があります。IoT システムの完全性リスクを評価するには、システムのデータが破壊されたり不適切に変更された場合の影響を評価します（低、中、高）。

可用性（I列）：システム情報が適時かつ確実にアクセス可能でなければならない度合いを評価するために、システム一定期間稼働できなくなった場合の潜在的なシステム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、可用性に関する特定のリスクが低、中、高を評価するために、*FIPS199*の「セキュリティ目的に対する潜在的影響の定義」と呼ばれる情報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後、IoTセキュリティコントロールフレームワークは、特定の環境に対して必要なすべてのセキュリティコントロールを特定することができます。

1 FIPS 199: "Standards for Security Categorization of Federal Information and Information Systems," Federal Information Processing Standards Publication, Computer Security Division, U.S. Department of Commerce; February 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

2 FIPS 200: "Minimum Security Requirements for Federal Information and Information Systems," Federal Information Processing Standards Publication, Computer Security Division, U.S. Department of Commerce; March 2006. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

影響レベルが高の場合は、低、中、高リスクレベルを含め、利用可能なすべてのセキュリティ対策を適用する必要があることに注意してください。影響レベルが中の場合は、中と低リスクのレベルに対するすべての対策を適用する必要があります。

以下は、3つの影響評価とそれに対応する必要なコントロールの例です。

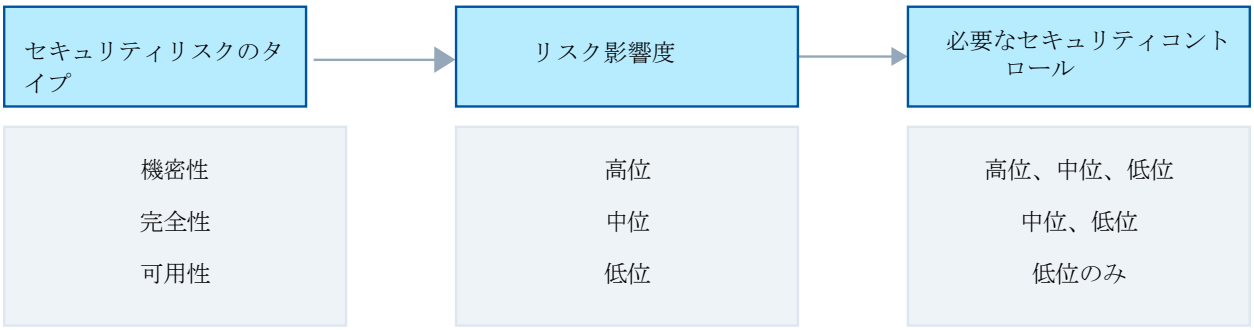


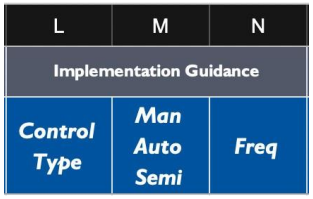
図2-CIAの例

補足的なコントロールガイダンス（J, K列）

追加の指示（J列）：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場合、特定の要求事項、用語の説明、役に立つ操作のヒントなどを詳述したこの補足情報を必ず参照してください。

参考資料（K列）：政府刊行物、規制情報、その他コントロール仕様を完全に理解し実施するために必要な参考資料など、専門的な情報についてはこのセクションを参照してください。

実施ガイダンス（L, M, N列）



企業のセキュリティ計画を実施する場合、「実施ガイダンス」のセクションを使用して、固有の環境に対するコントロールタイプを決定する（L列）。この洞察には、どのように、セキュリティ管理策を実施することができ（M列）、各セキュリティ管理策が実施されるべき頻度（N列）を示します。

セキュリティコントロールのタイプ（L列）

IoTフレームワークのセキュリティ対策は、「いつ」「どこで」「どのように」対策することでセキュリティを高めるかによって、3つのタイプに分類されます。

予防的管理策：何かが起こるのを防ぎます（例：鍵のかかったドアから部屋への物理的なアクセスを制限します、またはより高度な生体認証プロトコルを要求します）。

検知的管理策：インシデントを特定し、その特徴を把握します。例えば、実地調査後に在庫の不一致を調査する、ビデオを録画する、モーションセンサーを使用して不法侵入を検出する、などがあります。

是正的管理策：セキュリティインシデントによる被害を軽減します。例えば、消火器を使って火災の被害を抑える、プライマリデータセンターがクラッシュした場合に複製データセンターの可用性を確保する、などです。

コントロール実施ガイダンス（M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つの方法で実施されます。

手動型コントロール：人間が手動でコントロールします。例えば、リスクマネジメントのプロセスレビューでは、誰かがプロセスを評価し、ポリシーに従って実行されていることを確認します。

自動型コントロール：システムが人手を介さずに自動でコントロールします。例えば、ユーザーの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。その後、システムがその組み合わせを検証してからアクセスを許可します。

半自動型コントロール：半自動型コントロールは、自動型と手動型の対処を組み合わせたものです。例えば、実地棚卸では、物品を数え、その結果をシステムが作成したリストと比較します。その後、紙と電子の記録を含む調査によって、差異を調整します。

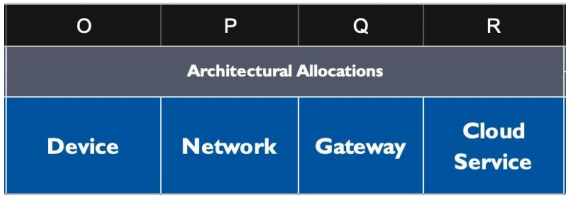
コントロールの実施頻度（N列）

組織によっては、内部リスクの優先順位や規制遵守の要件に基づき、より頻繁な統制を必要とします。以下の頻度は、様々な状況に対して推奨されます（個々の企業のニーズによって異なります）。

- Annually （毎年）
- Quarterly （四半期ごと）
- Monthly （毎月）
- Weekly （毎週）
- Daily （毎日）
- イベント毎：コントロール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）

デバイス、ネットワーク、ゲートウェイ、クラウドサービス（O, P, Q, R）

IoT Frameworkは、IoTシステムにおけるアーキテクチャ要素のコントロールの適用のガイドです。これらのアーキテクチャ要素は、次の図に示すように、IoTアーキテクチャ内の標準レイヤーを表します。



実装者は、これらの文書セクションを参照して、各レイヤーでコントロールが適用可能かどうかを判断する必要があります。各列では、IoTアーキテクチャ内に信頼境界を作成する機会について説明します。個別のコントロールを各レイヤーに適用する必要があります。

デバイス（O列）

デバイスレイヤによって処理、保存、生成されるデータに焦点を当てた，デバイスレイヤに直接適応されるコントロール。一般的なIoTデバイスには、センサ、アクチュエータ、および場合によっては最小限のユーザーインターフェースが組み込まれます。デバイスは、完全性を保護する必要のある構成ファイルを使用して、イベントまたはセキュリティログを収集および保存できる場合もあります。

ネットワーク（P列）

ネットワークレイヤでは、ワイヤレス通信アクセスポイント（WAP）などのコンポーネントがデバイスのWi-Fi接続をサポートします。他のネットワークコンポーネントには、ZigBeeなどのプロトコルをサポートするキー管理サーバが含まれる場合があります。さらに、ネットワークセキュリティコントロールは、ゼロトラスト設計、仮想ローカルエリアネットワーク（VLAN）セグメンテーション、ファイアウォール、および侵入検知で構成されている場合があります。データIoTネットワークを通過するときに、データの暗号化と完全性の保護を検討してください。

ゲートウェイ（Q列）

ゲートウェイレイヤでは、脅威アクターにとって、潜在的なIoTネットワークエントリポイントを意味します。ゲートウェイには、デバイスが通常実装するものを超える追加のセキュリティコントロールが適用される場合があります。

クラウドサービス（R列）

ほとんどのIoTデバイスは、クラウド環境で動作します。デバイスは、データをクラウドに直接送信することも、クラウドサービスを介して管理することもできます。クラウドに送信されるデータは、転送中およびクラウドプロバイダのストレージボリューム内で永続的に保護される必要があります。場合によっては、IDをIoTデータにリンクできないようにするため、クラウド内で匿名性保護を適用する必要があります。

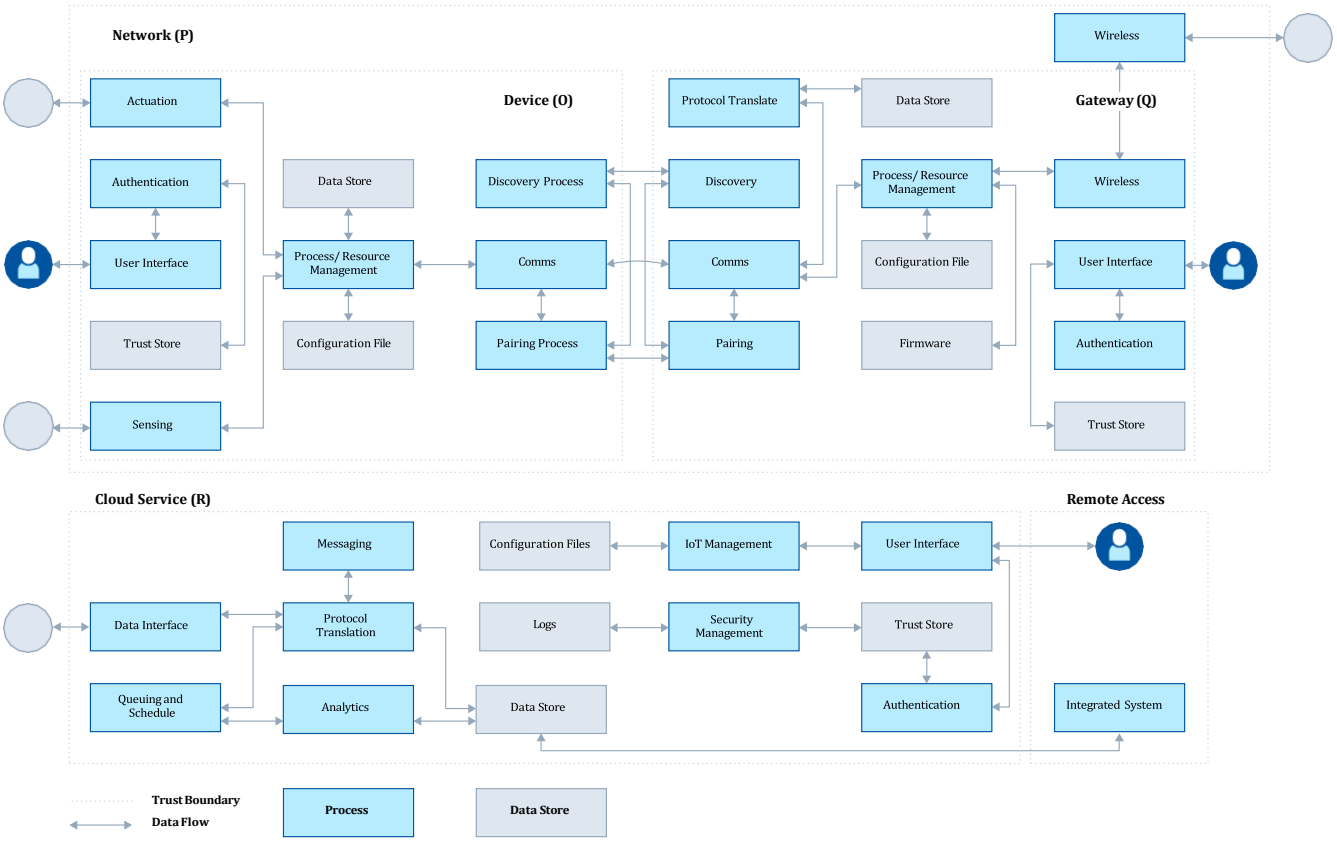


図3 - アーキテクチャ要素間のデータフロー

その他のリソース

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. “Foundational Cybersecurity Activities for IoT Device Manufacturers.” https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf May 2020. NISTIR 8259, National Institute of Standards and Technology.

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. “IoT Device Cybersecurity Capability Core Baseline.” https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf May 2020. NISTIR 8259A, National Institute of Standards and Technology.

Boeckl, Katie. Fagan, Michael. Fisher, William. Lefkovitz, Naomi. Megas, Katerina N. Nadeau, Ellen. Piccarreta, Ben. Gabel O’Rourke, Danna. Scarfone, Karen. “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.” https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf June 2019. NISTIR 8228, National Institute of Standards and Technology.

Iorga, Michaela. Feldman, Larry. Barton, Robert. Martin, Michael J. Goren, Nedim. Mahmoudi, Charif. “Fog Computing Conceptual Model: Recommendations of the National Institute of Standards and Technology.” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf March 2018. NIST SP 500-325, National Institute of Standards and Technology.

Interagency International Cybersecurity Standardization Working Group. “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT).” https:// nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf November 2018. NISTIR 8200, National Institute of Standards and Technology.

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

European Union Agency for Cybersecurity (ENISA). “Good Practices for Security of IoT: Secure Software Development Lifecycle.” https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 November 2019.

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

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

Microsoft Azure. “Security best practices for Internet of Things (IoT).” https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices October 2018.