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　バージョン2

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for Cloud Security Alliance Internet of Things research is https://cloudsecurityalliance.org/working-groups/internet-of-things/

Acknowledgments

Initiative Leads:

Aaron
Guzman
Michael
Roza Brian
Russell

Contributors:

Renu
Bedi
Ramon
Codina
Umesh
Jaiswal
Raj
Sachde
v
Ashish Vashishtha

CSA:

Hillary Baron
AnnMarie Ulskey (Graphic Design)

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　バージョン 2」は、Cloud Security Alliance (CSA)が公開している「CSA Guide to the IoT Security Controls Framework Version 2」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
2021 年 05 月 30 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 セキュリティコントロールフレームワーク利用ガイド　バージョン 2」の日本語訳は、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）

笠松　隆幸
勝見　勉
諸角　昌宏
山下　亮一

Table of Contents

はじめに

モノのインターネット（IoT）市場は、接続性（connectivity）と自律性（autonomy）の面での新たな進化を伴って様々な業界にわたって拡大を続けています。IoTで生成されたデータと機能に頼る度合いは急速に高まっており、これらの新しいテクノロジーを採用する企業組織は、アクセス可能で、安全で、レジリエンスのある配備を考える必要があります。技術の相互接続が急速に進むことと新しい脅威の絶え間ない流れを考えると、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、適切な対策を適切に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アーキテクチャについて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IoTシステムをセキュアに評価して実装するためにIoTセキュリティコントロールフレームワークをどのように使えばいいかについて説明しています。

IoT セキュリティコントロールフレームワークは、エンタープライズIoTシステムに関するものです。IoTシステムは、接続されたデバイスと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の多様な組み合わせです。IoT セキュリティコントロールフレームワークは、影響の可能性が限られた「価値の低い」データのみを処理するシステムから、重要なサービスを支える機密性の高いシステムまで、多くのIoTの領域にわたって有効です。システムの所管者は、保存され処理されるデータの価値と、さまざまな物理的セキュリティの脅威による影響の度合いに基づいてコンポーネントを分類します。

IoT セキュリティコントロールフレームワークは、ユーザが適切なセキュリティコントロールを選択し、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に適用されるコントロールは、最良のセキュリティ対応を示すものです。アーキテクチャコンポーネントによっては、フレームワークにある特定の推奨コントロールを実装できない場合があります。そのような場合、システムセキュリティアーキテクトはこれらの欠点を見つけ出し、代替手段を用いて残存リスクを軽減する案を考える必要があります。

ゴール

IoT セキュリティコントロールフレームワークは、実装を評価するため、また開発ライフサイクルを通じてセキュリティが進化するのを評価するためのツールを提供し、業界ごとに固有のベストプラクティスを確実に満たすようにします。

対象ユーザ

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エコシステムの設計を担当するシステムアーキテクト、開発者、およびセキュリティエンジニア向けのリソースです。監査人や侵入テスト実施者などのIoTシステム評価者は、IoT セキュリティコントロール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）を検証できます。

バージョンについて

バージョン1のIoT セキュリティコントロールフレームワークには、IoTシステムがさまざまな脅威環境で動作する際に直面する多くのリスクに対応するために必要な155の基本レベルのセキュリティコントロールが導入されています。

バージョン2のIoT セキュリティコントロールフレームワークには、バージョン1フレームワークを進化させて、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の割り当てを最小限に抑えます。重要な変更には、以下のページで説明する新しいドメイン構造とインフラストラクチャの開発が含まれます。

- コントロールの更新：すべてのコントロールを、技術的に明確にするために見直し更新しました。
- 新しいドメイン構造：各コントロールをより適切に分類するために、コントロールドメインを見直し更新しました。
- 新設の法的ドメイン：法令に関連するコントロールを導入しました。
- 新設のセキュリティテストドメイン：適用対象のコンポーネント（EXCEL シートでは architectural allocations 列）のセキュリティテストを導入しました。
- インフラストラクチャの割り当ての簡素化：デバイスタイプを単一のカテゴリに統合し、アーキテクチャコンポーネントへのコントロールの配備を簡略化しました。

将来の課題－バージョン3：以下の注目すべき改良を加える予定です：

- IoTフレームワークの責任共有マトリックス
- 安全（Safety）に特化したコントロール
- 侵入痕跡を示す情報
- ENISA（欧州ネットワーク情報セキュリティ機関）の IoT セキュリティガイドラインに対応した IoT フレームワーク
- ·米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（CSF）への IoT フレームワークおよび SP800-53 へのマッピング

IoTセキュリティコントロール フレームワークの使い方

下図1はCSA IoTセキュリティフレームワークの利用者が独自環境の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。

日本語版注意）カラムS（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。カラムSのフィルター機能を使うことで、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。

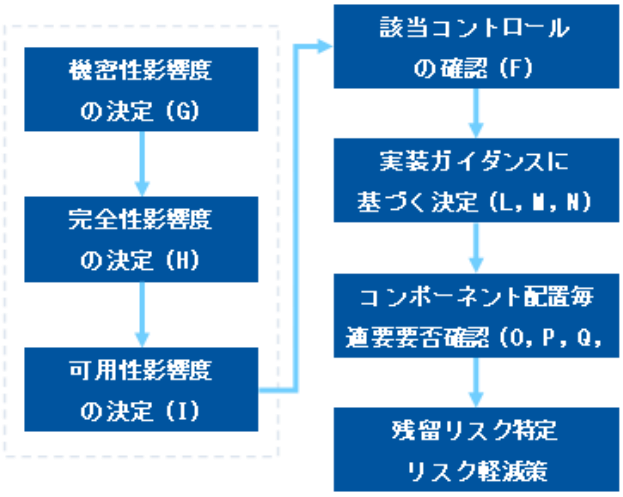


図1

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レベル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、および可用性について影響度の決定が行われると、フレームワークをフィルタリングし、それらの影響度に適用可能なコントロールのみを表示することができます。

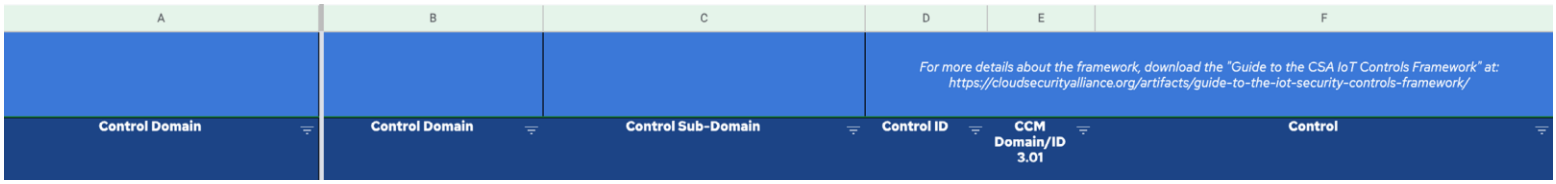
フレームワークをフィルタリングした結果の各コントロールを列Fで確認し、列Jで追加のガイダンスを確認します。列 O, P, Q, Rには、様々なコンポーネント配置によりコントロールを適用する必要があるかどうかが示されています。

これらの列により、利用者はデバイス、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という観点でコントロールをフィルタリングできます。

利用者は、列 L, M, Nを用いて各コントロールを実装する方法も確認できます。これらの列は、コントロールタイプ、コントロールを手動、自動、または両方の組み合わせのいずれかの方法を適用するか、コントロールを実行する頻度が示されています。

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、セキュリティーアーキテクトは、残存リスクを理解し、そのリスクを軽減するための補完的コントロ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（列 A, B, C, D, E, F）



コントロールドメイン（列 A）：個々のセキュリティ管理策の論理グループ（**下表参照**）によって編成され、列 F（コントロールの内容）に詳細が示されています。対応する管理策名は、コントールドメインのカテゴリ下に示されています。

コントロールドメイン（列 B）： ドメインはフィルタリングのために分類することができます。

コントロールサブドメイン（列 C）： サブドメインにより、更に細かな粒度でフィルタリングすることができます。

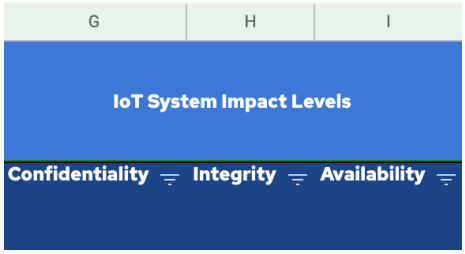
#	ドメイン（管理策名）	略号	サブドメイン
1	資産管理	ASM	命名規則、資産目録、資産監視
2	構成管理	CCM	設定ファイル、ファームウェアの更新、構成制御、EOL（End of Lile）管理計画
3	安全な通信	COM	信頼できるコミュニケーション、MQTT（Message Queuing Telemetry Transport）セキュリティ、暗号化された通信
4	安全なデータ	DAT	データ格付と分類、データクレンジング、保存されている暗号化されたデータ
5	ガバナンス	GVN	ガバナンスフレームワーク、規制および法的要件、コンプライアンス管理、プライバシー、事業継続性、安全性
6	IDおよびアクセス管理	IAM	パスワード管理、認証、承認、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	インシデント対応
8	IoTデバイスセキュリティ	IOT	認定デバイス、安全なプラットフォーム、安全な構成
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

#	ドメイン（管理策名）	略号	サブドメイン
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、イベント定義、無線周波数（RF）モニタリング
11	運用上の可用性	OPA	メンテナンス、フェイルオーバー、分散型サービス拒否（DDoS）保護、サービスレベルアグリーメント（SLA）
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	ポリシー策定、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、法定責任
15	安全なアプリケーション	SAP	モバイルアプリケーション、クラウドサービス、自律システム
16	安全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、安全な開発慣行、セキュリティテスト
17	安全なネットワーク	SNT	安全な検出、ネットワークの強靭化、ゼロトラストアーキテクチャ、ネットワークの視覚化
18	安全な無線通信	SWS	RF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
19	トレーニング	TRN	管理者トレーニング、ユーザートレーニング
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、アップデートとパッチ適用
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（列 D）：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識別子です。ID（「RSM-01」など）により、フレームワーク内の他の場所からそれが示すコントロールを参照することができます。

CCM ID （列 E)：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 CCM（Cloud Controls Matrix）から派生するか、関連している場合に、この列よって、一つ以上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、各フレームワークのコントロール内容の一部または全部をカバーします。

コントロールの記述（列 F）：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記述されています。使いやすさを考慮し、各コントロールは固有のIoT環境に対応できるよう、単純化されたアクションに分けられています。IoTシステムのリスク影響度(列G、H、I)



列 G から I:この情報により、ユーザ固有の環境に合わせてセキュリティ制御を初期調整ができます。個々のセキュリティ管理を調整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)と「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)を見直す必要があります。FIPS 199 と 200 の出版物では、リスク影響度を、機密性、完全性、可用性の 3 つの要素で、「低位、中位、高位」に分類しています。

機密性（列 G): 個人情報や独自の情報など、IoT システムの一部のデータは、適切な機密を保持するために、さまざまなセキュリティ制御を介したアクセス制限を必要とします。IoT システムの機密保持リスクのコンポーネントを評価するには、システム 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（低位、中位、高位）を見積もる必要があります。

完全性（列 H): データの完全性を保護する場合、企業は不適切なデータの変更や破壊を防ぐ必要があり、情報の信頼性を保証する必要がある。IoT システムの完全性リスクを評価するには、システム データが破壊された場合や不適切に変更された場合の影響（低位、中位、高位）を評価します。

可用性（列 I): システム情報が、タイムリーかつ信頼性の高い方法でアクセス可能な状態を維持する必要が、どの程度あるかを評価するために、システムが任意の期間動作不能になった場合に、システムの潜在的なリスクを評価します。

システム情報の機密性、完全性、可用性に関する特定のリスクが、低位か、中位か、高位かを評価するには、「FIPS 199の6ページ（*訳注： IPAの翻訳版では10ページ*）の「セキュリティ目的に対する潜在的影響の定義」を参照します。

これらのリスク影響度を決定した後、IoT セキュリティ制御フレームワークは、特定の環境に必要なすべてのセキュリティ制御を識別できます。

注意　影響レベルが高位の場合は、低位、中位、高位のリスク影響度を含め、利用可能なすべてのセキュリティ制御を適用する必要があります。影響度が中位の場合は、すべてのコントロールを中位、低位のリスク影響度に適用します。

[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

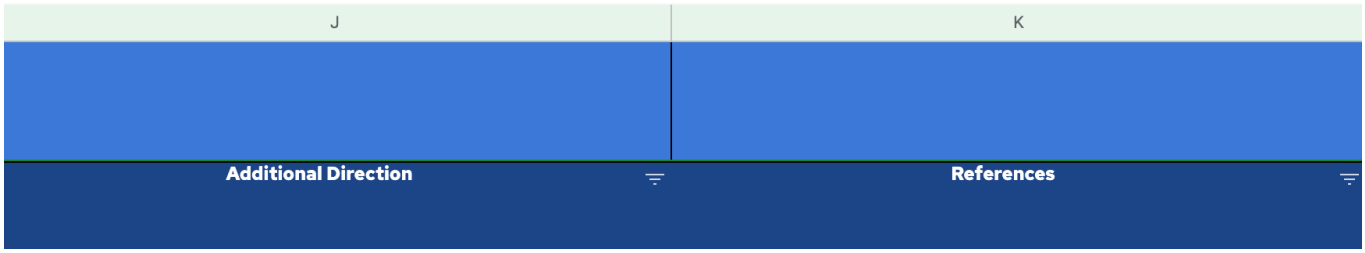
[2] FIPS 200: “Minimum Security Requirements for Federal Information and Information Systems,” Federal Information Processing Standards Publication, Computer Security Division, U.S. Department of Commerce; March 2006. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

以下の図は、3つの影響度と関連する管理策の例です。

リスクインパクトのタイプ	リスク影響度	セキュリティ管理策
機密性	高位	高位、中位、低位
完全性	中位	中位、低位
可用性	低位	低位のみ

図 2

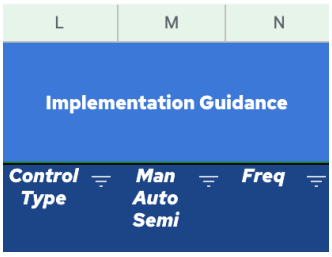
補足制御ガイダンス（列 J, K）



追加の指示（列 J）：IoT セキュリティ制御フレームワークで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は、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しく説明する補足情報を必ず参照します。

参考資料（列 K）：政府の出版物や規制情報など専門的な情報源、および制御仕様を完全に理解し実装するために必要なその他の資料は、このセクションを参照します。

実装ガイダンス（列 L、M、N）



企業のセキュリティ計画を実装する場合は、フレームワークの「実装ガイダンス」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します（列 J）。このフレームワークから導かれた決定には、組織がコントロールを実装する方法（列 K）と、各セキュリティ制御対策を施行する頻度（列 L）が含まれています。

セキュリティコントロールのタイプ（列 L）

“IoT Framework” のセキュリティコントロールは、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。

予防的管理策： 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。

検知的管理策： インシデントを特定し、特徴づけします。 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の使用などがあります。

是正的管理策： 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が停止した場合のセカンダリデータセンタの可用性など、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ガイダンス（列 M）

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： 人間が手動でコントロールします。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。たとえば、ユーザアクセスの検証において、ユーザはユーザ名とパスワードでログインします。それに対して、システムはアクセスを許可する前にその組み合わせを検証します。

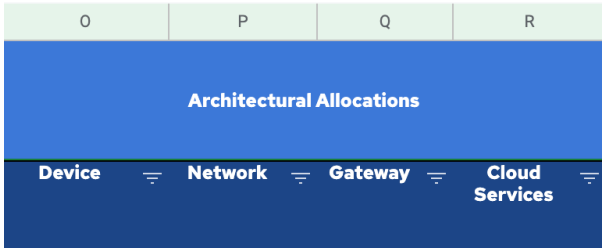
半自動型コントロール： 半自動型コントロールは、自動型と手動型の対処を組み合わせたものです。たとえば、現物在庫では、品目がカウントされ、結果がシステムが生成したリストと比較されます。相違があれば調査して是正しますが、その際、紙ベースと電子的記録の両方を利用します。

管理策の実施頻度（列 N）

組織によって、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（個々の企業のニーズに依存します）。

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

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を表します。

実装者は、これらの文書の各部を参照して、各レイヤ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に適用する必要があります。

デバイス（列 O）

デバイスによって処理、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用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インターフェイ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（列 P）

ネットワークレイヤでは、ワイヤレスアクセスポイント（WAP）などのコンポーネントがデバイスのWiFi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。データが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（列 Q）

ゲートウェイは、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（列 R）

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に、クラウド内で匿名性保護を適用する必要があります。

次の図は、これらのアーキテクチャレイヤを視覚的に表したものです。

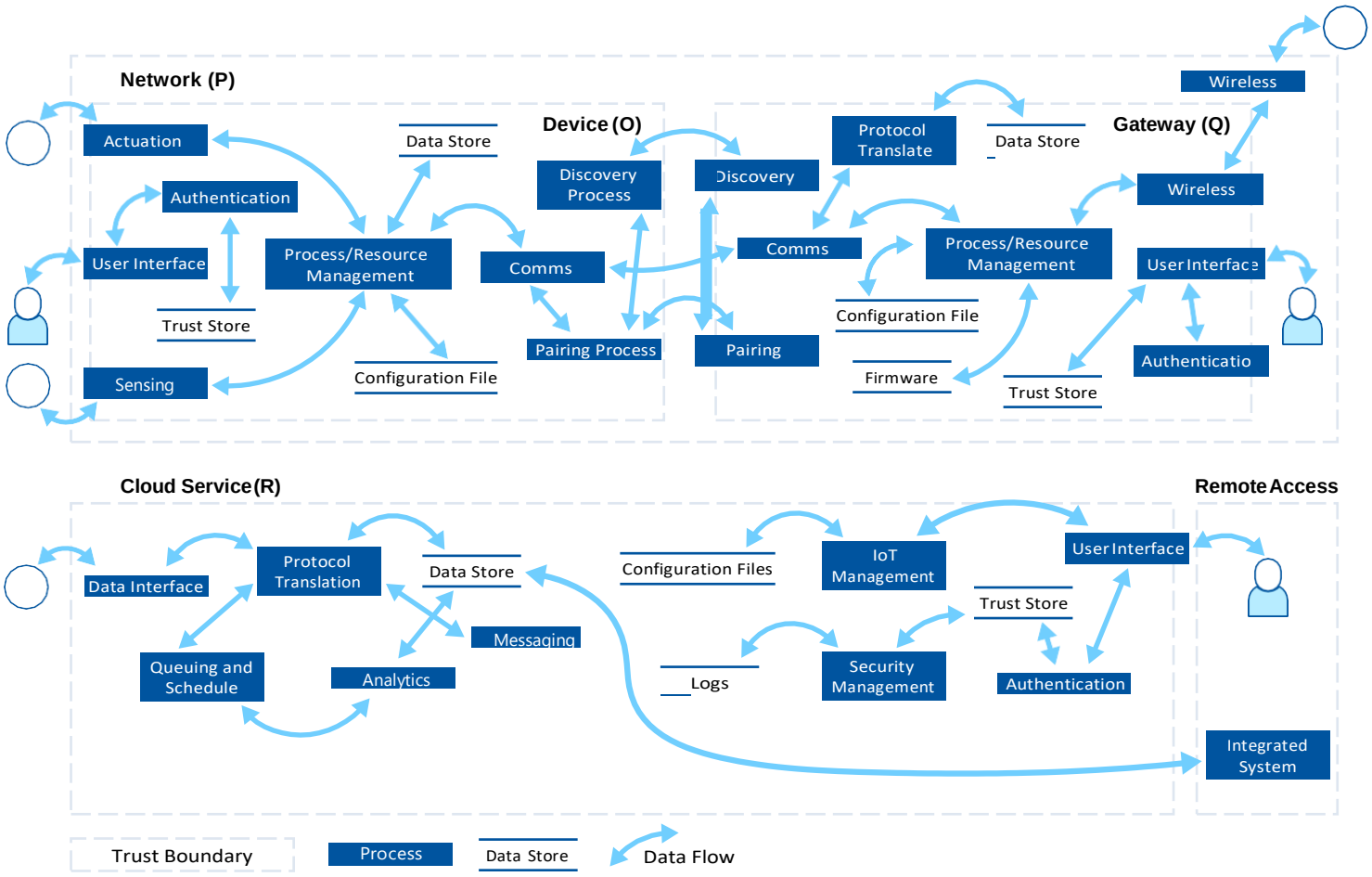


図3

Additional Resources

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.