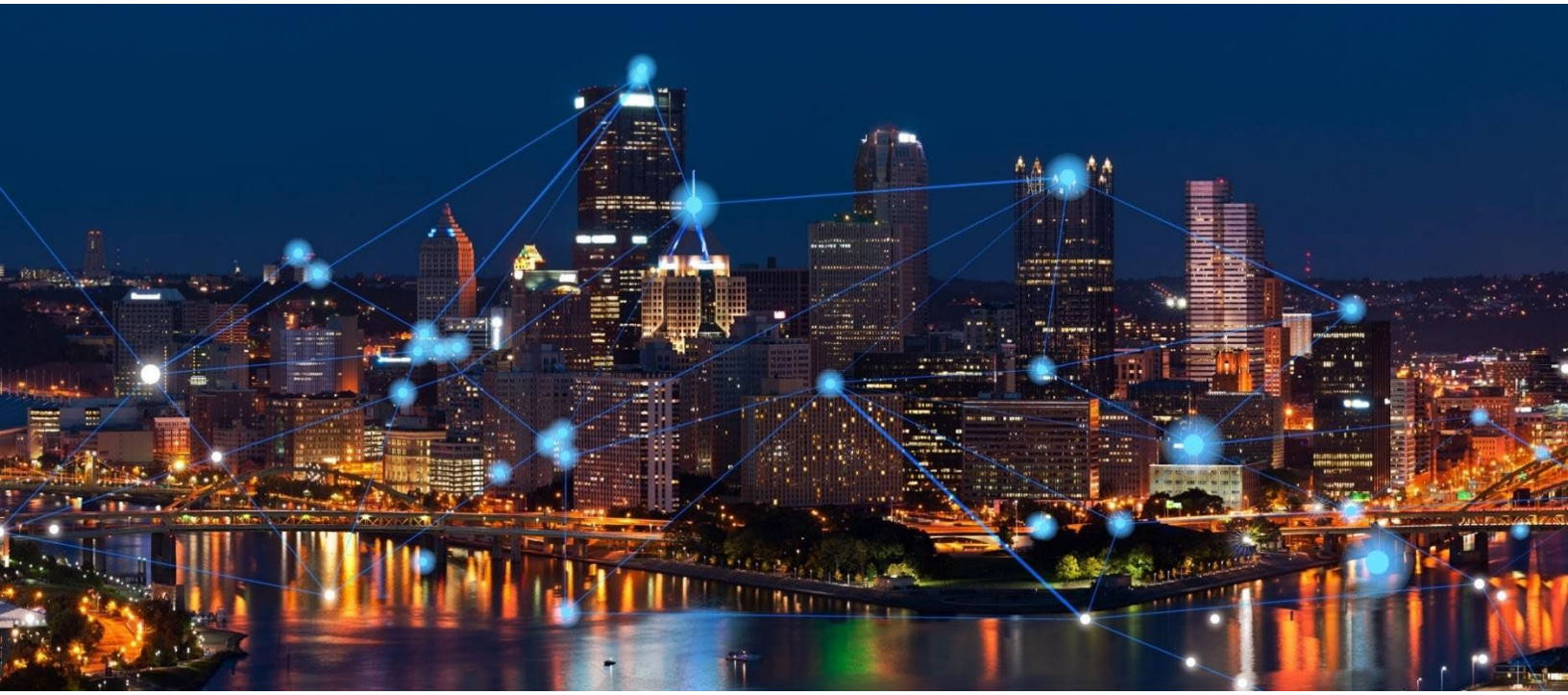
TLP:CLEAR



OTサイバーセキュリティの基礎：所有者および運用者向けの資産インベントリガイダンス

発行日：2025年8月13日

米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）
米国環境保護庁（EPA）
米国国家安全保障局（NSA）
米国連邦捜査局（FBI）
オーストラリア通信電子局傘下のオーストラリア・サイバーセキュリティセンター（ASD's ACSC）
カナダ サイバーセキュリティセンター（Cyber Centre）
ドイツ連邦情報セキュリティ局（BSI）
オランダ国立サイバーセキュリティセンター（NCSC-NL）
ニュージーランド国立サイバーセキュリティセンター（NCSC-NZ）

本文書はTLP:CLEARとマーキングされている。開示に制限はない。情報源は、公開に関する適用される規則および手順に従い、情報の悪用について予見可能なリスクが最小限または存在しない場合に、TLP:CLEARを使用してもよい。標準的な著作権規則に従うことを条件として、TLP:CLEARの情報は制限なく配布してもよい。トラフィックライトプロトコルに関する詳細については、トラフィックライトプロトコル（TLP）の定義と使用法 を参照のこと。

TLP:CLEAR

エグゼクティブサマリー

現代的な防御可能なアーキテクチャを構築する際、すべての重要インフラ分野における制御・運用技術（OT）の所有者および運用者は、OT分類体系（taxonomy）によって補完されたOT資産インベントリを作成することが不可欠である。これらのツールを活用することで、所有者および運用者は、自組織の環境内のどの資産をセキュア化及び防御すべきかを識別し、それに応じて防御体制を構築することで、サイバーセキュリティインシデントが組織のミッションおよびサービスの継続性に及ぼすリスクを低減できる。

資産インベントリとは、組織のシステム、ハードウェアおよびソフトウェアを体系的に整理し、定期的に更新されるリストである。OT環境において、資産インベントリを作成する上で重要な要素となるのが、OT分類体系を策定することである。これは、機能および重要度に基づいて資産を分類することにより、OT資産を整理および優先順位付けし、リスクの識別、脆弱性管理およびインシデント対応を支援する分類体系である。

本ガイダンスは、OTの所有者および運用者が資産インベントリおよびOT分類体系を作成するためのプロセスを概説する。このプロセスには、インベントリの範囲および目的の定義、資産の識別、属性の収集、分類体系の作成、データ管理、および資産ライフサイクル管理の実装が含まれる。これらのステップは、OT資産インベントリおよびOT分類体系を作成および維持するための徹底的かつ体系的なアプローチを定義しており、組織がOT資産に関する正確かつ最新の記録を維持することを可能にする。

さらに、本ガイダンスでは、OTの所有者および運用者が、最も重要な資産を防御するために、資産インベントリをどのように維持、改善、活用できるかを概説する。そのステップには、OTのサイバーセキュリティおよびリスクマネジメント、保守および信頼性、パフォーマンスの監視および報告、トレーニングおよび意識向上、ならびに継続的改善が含まれる。これらの分野に取り組むことで、組織は全体的なセキュリティ態勢を強化し、OT環境の信頼性および安全性を確実にすることができる。

OT分類体系の実例を示すため、CISAはエネルギー分野および上下水道分野の組織との作業会合を通じて、概念的な分類体系を策定した（**附属書B：石油・ガス組織向け分類体系**、**附属書C：電力組織向け分類体系**、および**附属書D：上下水道向け分類体系**を参照）。これらは各分野における権威ある分類体系ではないが、各分野の組織が独自の資産分類システムを策定するための指針となることを意図している。

Translation statement
This document was originally created by the Cybersecurity and Infrastructure Security Agency (CISA). It was translated by a third party and neither CISA nor the U.S. Department of Homeland Security reviewed the translation. Neither CISA nor DHS are responsible for any errors or omissions relating to this translation. CISA has granted permission to IPA to use the CISA logo and related properties only in a translation which represents a faithful reproduction of the original, and for no other purpose. All other rights reserved. You can find the original version of this document at CISA.gov.
U.S. Cybersecurity and Infrastructure Security Agency

翻訳に関する免責事項
本文書は元々、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）によって作成されたものである。本文書は第三者によって翻訳されたものであり、CISAおよび米国国土安全保障省（DHS）は翻訳内容を確認していない。CISAおよびDHSは、本翻訳に関する誤りや欠落について一切の責任を負わない。CISAはIPAに対し、原文を忠実に再現した翻訳においてのみ、CISAのロゴおよび関連する資産を使用することを許可しており、それ以外の目的での使用は認められていない。その他のすべての権利は留保されている。本文書の原文はCISAのウェブサイトで閲覧できる。
米国サイバーセキュリティ・インフラストラクチャセキュリティ庁

目次

はじめに 4
謝辞 6
OT分類体系 6
OT資産インベントリおよび分類体系を作成するためのステップ 8
インベントリおよび分類体系作成後の措置 11
OTサイバーセキュリティおよびリスクマネジメント 11
保守および信頼性 12
パフォーマンスの監視および報告 13
トレーニングおよび意識向上 13
継続的改善 13
追加リソース 13
質問およびフィードバック 13
連絡先情報 14
免責事項 14
改訂履歴 14
附属書A：資産インベントリの項目 15
附属書B：石油・ガス組織向け分類体系 19
演習のステップ 19
附属書C：電力組織向け分類体系 23
演習のステップ 23
附属書D：上下水道 27
演習のステップ 27
参考文献 31

はじめに

制御・運用技術（OT）には、プロセス自動化、計装、サイバーフィジカル運用、および産業用制御システム（ICS）を網羅する一連の技術が含まれる。多くのOTシステムは、運用においてプロセスデータおよび傾向分析に依存する業務運用およびアプリケーションとの接続が一層進んでいる。これらの接続がセキュアに構築および統合されていない場合、サイバー攻撃者がネットワーク間を移動するための経路となる恐れがある。

OTは、エネルギーの生産および供給、上下水道処理といった重要インフラサービスにとって不可欠であり、システムおよびサービスの妨害または破壊、あるいは恐喝などの悪質な活動を行おうとする悪意のあるサイバー攻撃者にとって、格好の標的となっている。OTサイバーインシデントは、金銭的損失、業務の中断、環境および健康ならびに人の安全の侵害など、OTの所有者および運用者に対して深刻な結果をもたらす可能性がある。サイバー攻撃者は、以下の悪用を含む複数の方法でインシデントを引き起こす可能性がある。

- OTシステムへのアクセスを得るため、欠陥のあるまたは古いソフトウェア／ファームウェアの**脆弱性**を悪用する。
- OTシステムへの不正アクセスを得るため、**脆弱な認証メカニズム**を悪用する。
- IT環境からOT環境へ、およびOTシステム間で横方向の移動を行うため、**不十分なネットワークセグメンテーション**を悪用する。
- 通信を傍受したり、悪意のあるコマンドを注入したり、産業プロセスを妨害または操作したりするため、**セキュアでないOTプロトコル**を悪用する。
- OTシステムへのアクセスを得て横方向の移動またはコマンド＆コントロールを行うため、**セキュアでないリモートアクセスポイント**を悪用する。

資産インベントリの作成は、現代的な防御可能なアーキテクチャを構築するために必要であり、CISAのサイバーセキュリティパフォーマンス目標（CPGs）の一つである。[1] 現代的な防御可能なアーキテクチャは、OTのサイバー防御担当者がサイバー脅威を識別、防止、および対応できるようにするとともに、信頼性、業務の継続性、安全性、および規制要件への準拠を確実にしつつ、十分に検討されたシステム設計および実装を通じてリスクを軽減する。[2] **OT資産インベントリ**（組織のOTシステム、ハードウェア、およびソフトウェアを体系的に整理し、定期的に更新されるリスト）は、現代的な防御可能なアーキテクチャを設計するための基盤となる。これは、インベントリがなければ、組織は自らが何を保有しており、何をセキュア化し保護すべきかを把握できないためである。

資産インベントリの作成は、OTの所有者および運用者が資産を識別、分類、文書化する、複数のステップからなるプロセスである。インベントリ作成プロセスの一環として**OT分類体系**を作成するOTの所有者および運用者は、このプロセスを大幅に効率化できる。OT分類体系とは、リスクの識別、脆弱性管理、およびインシデント対応を円滑に行うために、OT資産を整理し優先順位をつけるために用いられる分類システムである。

---

[1] CISAのCPGは、CISAおよび米国国立標準技術研究所（NIST）がすべての組織に実装を推奨する、プラクティスおよび保護策の最低限のセットを規定している。CISAおよびNISTは、最も一般的かつインパクトの大きい脅威、戦術、技法、および手順から組織を保護するため、既存のサイバーセキュリティフレームワークおよびガイダンスに基づいてCPGを策定した。追加で推奨されるベースライン保護策を含むCPGに関する情報については、CISAのCPGウェブページを参照のこと。

[2] 現代的な防御可能なアーキテクチャに関する情報については、ASD ACSCの Modern defensible architecture を参照のこと。

この分類体系は、資産を機能および／または重要度ごとに分類し、資産間の関係および依存関係を可視化することを容易にすることで、所有者および運用者による資産インベントリの実施を支援する。

本ガイドは、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）および以下のパートナー[3]によって作成されたもので、資産インベントリを作成するための主要要素およびベストプラクティス、ならびにOT分類体系を作成するための業界で認められたアプローチを紹介している。

- 米国環境保護庁（EPA）
- 米国国家安全保障局（NSA）
- 米国連邦捜査局（FBI）
- オーストラリア通信電子局（ASD）傘下のオーストラリア・サイバーセキュリティ・センター（ACSC）
- カナダ・サイバーセキュリティセンター（Cyber Centre）
- ドイツ連邦情報セキュリティ局（BSI）
- オランダ国家サイバーセキュリティセンター（NCSC-NL）
- ニュージーランド国立サイバーセキュリティセンター（NCSC-NZ）

本ガイドでは、潜在的な脅威に先手を打つために、先を見越した計画立案、ITチームとOTチーム間の連携、および可能かつ適切な場合には最先端技術の統合の重要性を強調している。OTの状況は絶えず変化している。本ガイドは、考えられるすべてのOT資産について包括的な見解を提供することを意図したものではない。むしろ、本文書は、組織が既に保有しているOT資産インベントリのリソースを補完することを意図している。

また、本ガイドには、エネルギー分野の石油・ガス組織および電力組織、ならびに上下水道分野の組織を対象としたワーキングセッションを通じて作成された概念的な分類体系も含まれている（**附属書B：石油・ガス組織向け分類体系、附属書C：電力組織向け分類体系、附属書D：上下水道向け分類体系**を参照）。CISAは、2025年初頭に開催された8回の協働ワーキングセッションを通じて、これらの分類体系を作成した。 CISAは、米国連邦政府機関および民間分野の代表者を含む、約14の組織および33名の参加者からフィードバックを収集し、それを取り入れた。これらは、各分野に対する権威ある指示ではないが、OT資産を分類するための広く採用された手法を持たない分野固有の組織の指針となることを意図している。

作成組織は、所有者および運用者に対し、以下のことを推奨している。

- 「OT資産インベントリおよび分類体系を作成するためのステップ」のセクションに記載された推奨事項をレビューし、実装することで、資産インベントリのプロセスを改善すること。
- 本ガイドを、組織内で、および同業他社と共有すること。
- CISAの匿名の製品アンケートを通じて、本ガイドに対するフィードバックおよび今後のガイドに向けた提言を提供すること。

[3] 以下、「作成機関」と呼ぶ。

謝辞

CISAは、エネルギー省（DOE）およびOTの所有者および運用者を含むその他の政府および民間分野のパートナーと協力し、共同サイバー防衛連携（JCDC）[4]を通じて本ガイドの作成を主導した。

以下の業界ステークホルダーが、本書の作成に貢献した。

- American Water
- British Petroleum PLC
- Denver Water
- Duke Energy Corporation
- Energy Threat Analysis Center (ETAC)[5]
- Eversource Energy
- James Kimzey Regional Water District
- Lansing Board of Water & Light
- Loudoun Water
- Marathon Petroleum Corporation
- Montgomery Township Municipal Sewer Authority
- Pacific Gas & Electric Company
- Southern California Edison

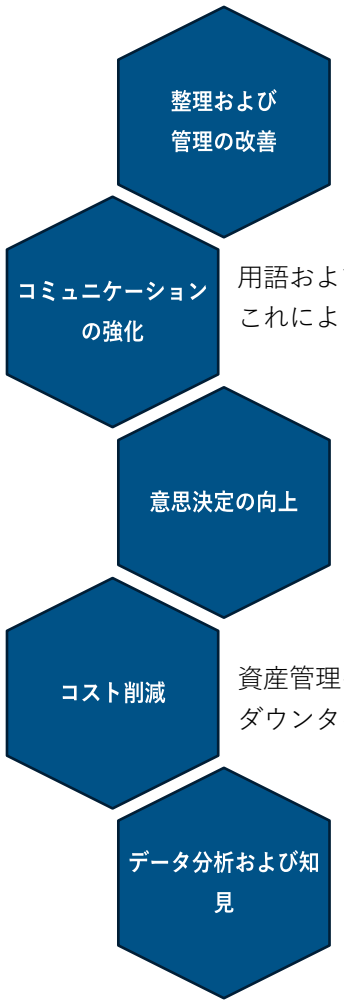
OT分類体系

正確かつ最新の資産インベントリを維持することは複雑である。OT環境には、レガシーシステム、専用デバイス、センサー、および計測機器など、多様な資産が含まれることが多い。これらの資産は、通信に様々な独自プロトコルを使用している。所有者および運用者は、物理プロセスの監視および制御における各コンポーネントの役割に関する文脈を把握する必要がある。そのため、所有者および運用者は、資産および関連するプロセスエリアを実際にレビューおよび点検しなければならない場合がある。

[4] JCDCは、CISA内の官民連携組織であり、2021年国防授権法（NDAA）において議会から付与された権限を活用し、サイバースペースの防衛に向けて世界的なサイバーコミュニティを結束させるものである。

[5] 米国エネルギー省と民間分野は、エネルギー分野における脅威の状況認識、緩和、および対応に関する運用上の連携を図るため、ETACを設立した。ETACは、電力情報共有・分析センター（E-ISAC）や国立研究所を含む産業界および政府の専門家を集め、非機密レベルおよび機密レベルの活動を通じて、米国のエネルギーシステムに対するサイバー脅威を識別し、対処している。

所有者および運用者は、この複雑さに対処するため、資産インベントリ作成プロセスにOT分類体系の作成を取り入れることが望ましい。OT分類体系は、コンポーネントおよびシステムに対する分類手法を提供し、資産インベントリの作成と維持管理を効率化する。OT分類体系を用いてOT資産インベントリを構築することの主な利点は以下の通りである。



適切に構成されたOT分類体系により、様々な資産、プロセス、およびデータを効果的に分類し、整理することができる。これにより、情報の管理および検索が容易になり、より効率的な業務につながる。

用語および分類を標準化することで、全員が同じ言語を使用することを確実にするのに役立つ。これにより、誤解が減少し、異なるチームおよび部門間の連携が向上する。

異なる資産およびプロセス間の関係および依存関係を明確に把握することで、組織はより適切な意思決定を行うことができる。これには、リソースの割り振りの最適化、保守計画の策定、およびアップグレードの実施が含まれる。

資産管理を最適化し、非効率性を低減することで、OT分類体系は大幅なコスト削減をもたらし、ダウンタイムを最小限に抑え、全体的な業務効率を向上させることができる。

構造化されたOT分類体系は、データを整理し分析するための明確なフレームワークを提供することで、より優れたデータ分析を可能にする。これにより、継続的な改善およびイノベーションを推進できる有益な知見が得られる。

OT資産インベントリおよび分類体系を作成するためのステップ

作成機関は、所有者および運用者がOT資産インベントリおよび分類体系を作成するにあたり、以下のステップを完了することを推奨している（**図1**参照）。

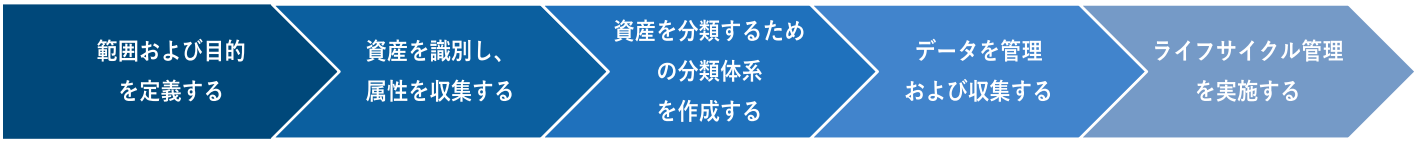


図1：資産インベントリのステップ

1. 範囲および目的を定義する。

a. **資産管理に関するガバナンスを定義する。**OT資産インベントリの作成を要求する権限者を識別する。組織内のどの部署または役職が、インベントリの作成および維持に責任を負い、かつ／またはその恩恵を受けるかを決定する。

b. **役割を割り当てる。**データの収集および検証に関する役割および責任を割り当てる。

c. **範囲を定義する。**プログラムの範囲（例：特定のゾーン、施設、システムおよび開発スケジュール）を設定し、インベントリにおいて「資産」を構成するものを識別する。

2. 資産を識別し、属性を収集する。

a. **資産を識別する。**システムコンポーネントに関する詳細なデジタル情報およびネットワークベースの情報を収集し、物理的な検査および論理的な調査を実施する。OT資産およびネットワークインフラの依存関係の包括的なリストを作成する。資産インベントリの範囲は、文書および物理的な検査で識別された資産を考慮に入れることが望ましい。

b. **資産の属性を収集する。**これらは、資産を記述するフィールドとしてインベントリに含めることが望ましい。以下の優先度の高い属性の収集を優先する（これらの属性の利点、および作成機関が収集を推奨するその他の属性については、組織にそれらを収集するリソースがある場合、**附属書A「資産インベントリのフィールド」**を参照のこと）。

i. 有効な／サポートされている通信プロトコル
ii. 資産の重要度
iii. 資産番号
iv. 資産の役割／種類
v. ホスト名
vi. IPアドレス
vii. ログ記録
viii. メディアアクセス制御（MAC）アドレス
ix. 製造業者
x. モデル
xi. オペレーティングシステム（OS）
xii. 物理的な場所／住所
xiii. ポート／サービス
xiv. ユーザーアカウント

3. 資産を分類するための分類体系を作成する。

分類体系を構築するには、5つのステップがある（**図2**参照）。**注：**エネルギー分野の石油・ガス組織および電力組織、ならびに上下水道部門の組織を対象としたワーキングセッションを通じてCISAが作成した分類体系については、

附属書B：石油・ガス組織向け分類体系、附属書C：電力組織向け分類体系、附属書D：上下水道向け分類体系を参照のこと。

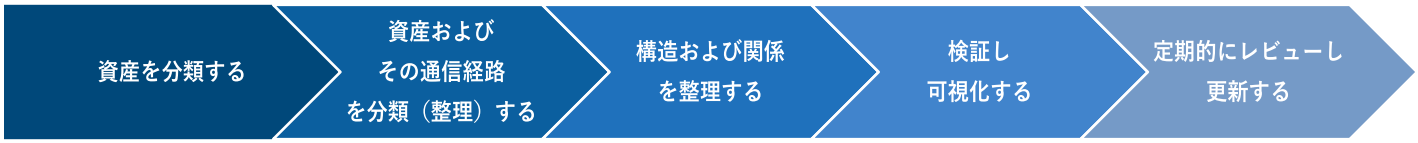


図2：OT分類体系の構築方法

a. **資産を分類する。**OT資産を分類するための一般的な方法には、重要度または機能に基づくものがある。

   i. **重要度に基づく分類**

      (1) 資産は、組織の業務、安全、およびミッションに対する重要度に基づいて分類される。

      (2) 重要資産とは、その障害または侵害が最も重大なインパクトを及ぼす資産のことである。

   ii. **機能に基づく分類**

      (1) 資産は、制御システム、通信デバイス、監視ツール、エンジニアリング、保守、または管理機能など、OT環境内での役割や露出度に基づいてグループ化される。

      (2) このアプローチは、依存関係および相互接続性を理解するのに役立つ。

b. **資産およびその通信経路を分類（整理）する。**

   注：資産や通信経路等を整理するためのモデルおよび規格は複数存在し、その選択は組織の裁量に委ねられている。 CISAが、**附属書B：石油・ガス組織向け分類体系、附属書C：電力組織向け分類体系、附属書D：上下水道向け分類体系**の分類体系を作成するために使用した国際自動制御学会（ISA）／国際電気標準会議（IEC）の62443シリーズの規格では、資産をゾーン（Zone）およびコンジット（Conduit）に分類している。[6]

   i. **ゾーン**とは、重要度や結果などの要因に基づき、共通のセキュリティ要件を共有する論理的または物理的な資産（例：制御資産、安全資産、非武装地帯［DMZ］内の資産）のグループである。例えば、生産ラインを制御するすべての機械は、同じレベルの保護を必要とするため、1つのゾーンに属する可能性がある。ゾーンは、類似した資産のセキュリティ確保に焦点を当てるのに役立ち、現在のセキュリティケイパビリティを定められた要件と照らし合わせることができる。

   ii. **コンジット**とは、通信専用であり、かつ同一のサイバーセキュリティ要件を共有するサイバー資産のグループである。コンジットは、認可されたデータまたはトラフィックのみがゾーン間を通過できることを確実にする。例えば、コンジットは工場の制御システムと監視システムを接続する場合があるが、不正アクセスを防ぐための厳格なルールが設けられている。

[6] *Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design.* International Society of Automation, 2020.

OTシステムは、複数のコンジットに同時に接続することができる。コンジットを特定するには、組織はデータフロー分析、プロトコルの識別、およびレイヤー2／レイヤー3のネットワーク詳細を取り入れながら、ゾーン間の通信経路をマッピングすることが望ましい。

c. 構造および関係を整理する。

i. プロセスの依存関係（例：操作シーケンスまたは制御フロー）を識別する。

ii. 階層全体にわたって明確さおよび一貫性を確実にするため、資産には一貫した命名規則を採用する。

iii. 命名規則の方法論、構造、および例外を含む詳細な文書を作成する。

iv. 資産に関与する役割および責任（オペレーター、技術者、ベンダー、インテグレーターなど）を文書化する（アクセスまたは認証情報に固有のものではなく、運用または保守などの機能の所有権について）。

d. 検証し可視化する。

i. 収集したインベントリの正確性および完全性を照合する。

ii. 資産カテゴリ（例：ゾーンおよびコンジット）を表す図を作成する。ゾーンおよびコンジットに整合した電力組織の分類体系の図の例については、**図3**を参照のこと。

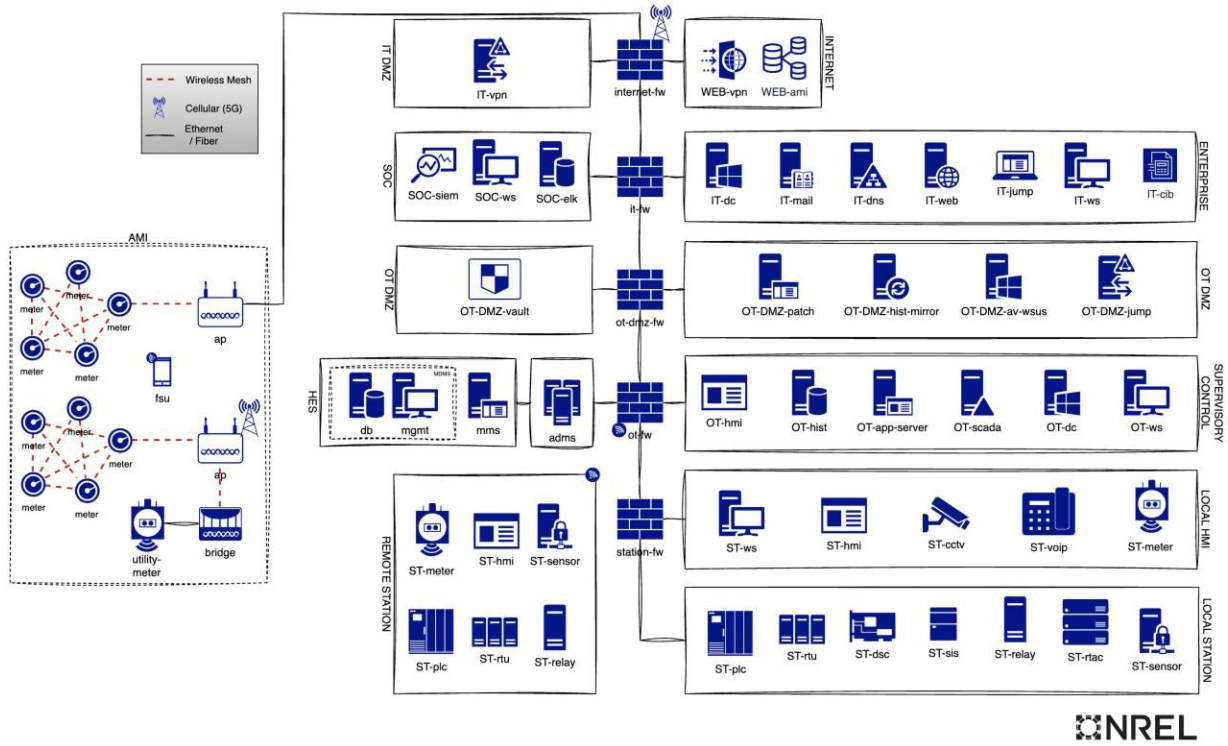


図3：配電環境の参照アーキテクチャの例[7]

[7] 米国国立再生可能エネルギー研究所（NREL）提供。

iii. 資産間の関係や依存関係を示すために、表または図を使用する。

e. **定期的にレビューし更新する。**

i. 技術や運用上の変化を反映させるため、分類体系を定期的にレビューし、更新する。

ii. 分類体系がステークホルダーのニーズを満たし、OT環境を正確に表現していることを確実にするために、ステークホルダーからフィードバックを収集する。

4. **データを管理および収集する。**

a. **追加の資産情報源を識別する。**インベントリを充実させる可能性のある各資産のデータソース（例：インテグレーターとの合意、ベンダーのマニュアルおよびハンドブック、保守記録、記録された運用データ、構成仕様書）を識別し、それらを含めることについて費用対効果分析を行う。

b. **データを保存する。**追加の資産データを保存および管理するための一元化されたデータベースまたは資産管理システムを確立し、サイバー脅威に対するデータ保護およびレジリエンスを確保するためのセキュリティ管理策を実装する。

5. **ライフサイクル管理を実施する。**

a. **ライフサイクルの段階を定義する。**各資産のライフサイクルの段階（例：取得、展開、試運転、保守、廃止）を定義する。

b. **ライフサイクルのポリシーを作成する。**保守スケジュール、交換計画およびバックアップ戦略を含め、ライフサイクル全体を通じて資産を管理するためのポリシーを作成する。これには、組織の変更管理プロセスに従うこと、および緊急変更権限の下であっても、システムへのデバイスの導入または削除には、いかなる場合でも資産インベントリの更新を必要とすることが含まれる。

インベントリおよび分類体系作成後の措置

以下のセクションでは、OTの所有者および運用者が自身のインベントリについて実施することが望ましい主要な措置について概説する。

OTサイバーセキュリティおよびリスクマネジメント

- ベンダーのシステムおよびアプリケーションについて、**既知の脆弱性**、利用可能なパッチ、更新プログラム、および堅牢化に関するガイダンス**を識別する。**
- **インベントリを**、積極的に悪用されている脆弱性を示しているCISAの既知の悪用された脆弱性（KEV）カタログや、識別されたセキュリティ上の欠陥に関する詳細なレポートを提供しているMITREの「Common Vulnerabilities and Exposures（CVE）」データベース[8]などの、確立された脆弱性データベースと**照合する。**
  - パッチを直ちに適用できない、またはサポート終了となっているベンダーのシステムおよびアプリケーションにおける既知のOT脆弱性に対するセキュリティ管理策を継続的に探索する。

[8]「Common Vulnerabilities and Exposures (CVE)」。cve.org。2025年6月24日閲覧。https://www.cve.org/。

  - 重要な資産およびシステムを優先順位付けし、それらの脆弱性が標的となった場合の冗長化計画および侵害された状態で運用する能力を詳細に示す。
  - 新たな脅威や脆弱性を検知するために、リアルタイム監視を実施する。
  - KEVカタログを、脆弱性管理の優先順位付けフレームワークにおける信頼できる情報源として使用する。ステークホルダー固有の脆弱性分類（SSVC）モデルなどの脆弱性管理フレームワークは、脆弱性の悪用状況を考慮している。組織はまた、KEVの脆弱性を自動的に取り込み、フラグを立てたり優先順位付けしたりする自動化された脆弱性およびパッチ管理ツールの使用も検討することが望ましい。
- 潜在的な攻撃パターンを、MITRE ATT&CK Matrix for ICS [9] や MITRE の共通攻撃パターン一覧および分類（CAPEC）：産業用制御システムパターン[10] などの既知の脅威インテリジェンス情報源にマッピングすることで、**脅威要因の優先順位付けを行う**。最も重大なリスクに基づいて、セキュリティの取り組みの優先順位付けを行う。
- セグメンテーション、アクセス管理および監視などの効果的な管理策を組み込んだセキュリティアーキテクチャを設計することで、**セキュリティ態勢を強化する**。

保守および信頼性

- 脆弱性アセスメントの結果および緩和策を考慮して、**保守計画をレビューする**。緊急性を要する変更が必要となる場合を除き、保守期間中に緩和措置またはパッチ適用の予定を決める。
- 潜在的なダウンタイムまたはサービス低下によるコストと、これらの脆弱なシステム（レガシーシステムの場合）を置き換えるコスト、あるいは代替管理策の導入にかかる**コストを比較する**。
- サイバーインフォームド・エンジニアリング[11]の原則およびセキュア・バイ・デザインのガイダンスを使用し、新しいシステムの調達およびエンジニアリング設計にセキュリティを組み込むことで、よりセキュアなシステムを実装する（共同ガイドSecure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Productを参照）。分類体系およびリスクマネジメントプロセスを活用し、セキュリティ上の意思決定の根拠とする。
- OT用予備コンポーネントのインベントリを分析し、その備蓄が、運用上の信頼性を確保するためにインベントリで識別された重要資産を十分にカバーしているかどうかを判断する。

---

9 「産業用制御システム Matrix」。MITRE ATT&CK®。2025年6月24日閲覧。https://attack.mitre.org/matrices/ics/。

10 「CAPEC VIEW：産業用制御システム（ICS）パターン」。MITRE。2025年6月27日閲覧。https://capec.mitre.org/data/definitions/703.html。

11 「Cyber-Informed Engineering.」アイダホ国立研究所（INL）。2025年6月24日閲覧。https://inl.gov/national-security/cie/.

パフォーマンスの監視および報告

- **資産のパフォーマンスおよび状態を継続的に監視する。**パフォーマンス上の問題または保守の必要性を検知するため、温度、圧力、流量などのリアルタイム指標に焦点を当てたプロセス変数の監視、および／または、通信の状態、デバイスの接続性、プロセスフローの完全性を分析する継続的な監視ツールを活用したネットワークおよびシステム診断の監視を優先する。
- 資産のパフォーマンス、保守活動、およびポリシーへの準拠状況を追跡するための**報告の仕組みを作成する。**
- OT資産インベントリの継続的な正確性、維持管理、および報告を確実にするため、更新を監督し、資産の分類を検証する**資産インベントリの所有者を識別する。**

トレーニングおよび意識向上

- 資産管理のプラクティス、ツール、および手順について、スタッフにトレーニングを行う。
- すべてのステークホルダーが資産管理の重要性を確実に理解できるよう、意識向上プログラムを実施する。

継続的改善

- 資産管理活動から知見を収集し、改善すべき領域を識別するための**フィードバックループを実施する。**
- OT資産の変更、追加、および廃止を正確に追跡するため、**変更管理プロセスを使用する。**
- インベントリの有効性が維持され、組織の目標と整合していることを確実にするため、資産管理プログラムの監査およびインベントリの**定期的なレビューを実施する。**

追加リソース

資産管理およびOTサイバーセキュリティに関する詳細については、以下のリソースを参照のこと。

- NISTのサイバーセキュリティフレームワーク
- CISAの 制御・運用技術（OT）サイバーセキュリティの原則
- CISAの サイバーセキュリティパフォーマンス目標（CPGs）
- EPAの 水道セクターサイバーセキュリティプログラムの事例研究：小規模下水処理システム

質問およびフィードバック

ステークホルダーは、CISAの匿名の製品アンケートを通じてフィードバックを提供することが推奨される。

連絡先情報

米国の組織は、本ガイドの情報に関連する不審な活動または犯罪行為を、以下に報告することが推奨される。

- CISAの24時間365日対応オペレーションセンター SOC@mail.cisa.dhs.gov または 1-844-Say-CISA (1-844-729-2472）、もしくは、最寄りのFBI支局。可能であれば、インシデントに関する以下の情報を含めること：インシデントの発生日時および場所、活動の種類、影響を受けた人数、活動に使用された機器の種類、報告を行う企業または組織の名称、および指定された連絡先。
- NSAのサイバーセキュリティガイダンスに関する問い合わせは、CybersecurityReports@nsa.gov まで連絡する。
- 上下水道システム分野の組織は、状況認識を自主的に提供するため、EPAの水インフラ・サイバーレジリエンス部門 watercyberta@epa.gov に連絡する。

オーストラリアの組織は、サイバーセキュリティインシデントを報告し、アラートおよびアドバイザリにアクセスするために cyber.gov.au にアクセスするか、1300 292 371（1300 CYBER 1）に電話する。

カナダの組織は、サイバーセンター contact@cyber.gc.ca 宛てにメールを送信してインシデントを報告する。

ドイツの組織は、サイバーセキュリティインシデントを報告するために bsi.bund.de/EN/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html にアクセスする。

オランダの組織は、アドバイザリについては ncsc.nl にアクセスし、NCSC-NL cert@ncsc.nl 宛てにインシデントをメールで報告する。

ニュージーランドの組織は、サイバーセキュリティインシデントを incidents@ncsc.govt.nz 宛てに報告するか、04 498 7654 へ電話する。

免責事項

本文書は、人命、健康、財産、または環境に対するリスクなど、OTの安全に関する事項については扱っていない。また、本文書は、ポリシーを策定したり、要件を課したり、措置を義務付けたり、既存の法的または規制上の義務に優先したりするものではない。本文書に基づいて行われるすべての措置は、任意のものである。

本報告書に記載されている情報は、情報提供のみを目的として「現状のまま」提供されている。作成機関は、本文書内でリンクされているものも含め、いかなる営利事業体、製品、企業、またはサービスについても推奨するものではない。サービスマーク、商標、製造業者、その他の方法による特定の営利事業体、製品、プロセス、またはサービスへの言及は、作成機関による推奨、推薦、または支持を構成するものでも、それを示唆するものでもない。

改訂履歴

2025年8月13日：初版。

附属書A：資産インベントリの項目

資産管理を成功させるには、インベントリ内の各資産について、どのようなデータを収集すべきかを理解する必要がある。表1は、推奨される資産インベントリの項目と、それらを含めることによる潜在的な利点を示している。

CISAの Malcolmを使用した監視および共通セキュリティアドバイザリフレームワーク（CSAF）[12]を使用した脆弱性管理に関する属性の詳細については、以下のリポジトリ[13]を参照のこと。

表1：資産インベントリの項目、属性、および要件の優先順位に関する推奨事項

資産インベントリの項目	属性の利点	優先度
有効な／サポートされている通信プロトコル	ネットワークトラフィックの分析に役立つ。 最初に、IT/OT境界外のデバイスと通信する資産または広域ネットワークを介して監視制御およびデータ収集（SCADA）デバイスと通信する資産に焦点を当て、その後、それらに該当しない資産に焦点を当てる。	高
資産の重要度	資産の運用上の役割、安全性へのインパクト、および／またはリスクへの露出に基づいて、資産を管理できるようにする。	高
資産番号	組織によって資産に割り当てられた一意の識別子。	高
資産の役割／種類	ネットワーク内の資産の文脈および機能を理解するのに役立つ。 資産の種類の一般的な例としては、次のようなものがある。 ▪ エンジニアリングワークステーション ▪ プログラマブル・ロジック・コントローラ（PLC） ▪ ヒストリアン ▪ ネットワークスイッチ／ルーター ▪ ハイパーバイザーホスト	高
ホスト名	ホストの命名規則に含まれている場合、ネットワーク内の資産の文脈および機能を理解するのに役立つ可能性がある。	高
IPアドレス	ネットワークトラフィックの分析に役立つ。	高

12 「Common Security Advisory Framework (CSAF)」、Oasis、2025年8月8日閲覧、https://www.csaf.io/。

13 「DINA-community/String-Sysiphos/Attributes of Data Model」、GitHub、最終更新日 2025年8月2日、https://github.com/DINA-community/String-Sysiphos/blob/main/datamodel/datamodel_attributes.md。

資産インベントリの項目	属性の利点	優先度
ログ記録	資産からのログがどのように収集されるかについての詳細を提供し、潜在的に悪意のある活動の検知および調査を可能にする。	高
MACアドレス	別途指定されていない場合、製造業者を特定するのに役立つ。（注：ネットワークカードの製造業者のみを指す場合がある。）	高
製造業者	既知の脆弱性を特定するのに役立つ。	高
モデル	既知の脆弱性を特定するのに役立つ。	高
オペレーティングシステム	該当する場合は、既知の脆弱性を特定するのに役立つ。	高
物理的な場所／住所	資産がどこにあるかに関する詳細を提供する。	高
ポート／サービス	役割の確認および攻撃対象領域の特定に役立つが、作成および維持には非常に時間がかかる。 最初に、OTセキュリティ境界外のデバイスと通信する資産または広域ネットワークを介して監視制御およびデータ収集 (SCADA) デバイスと通信する資産に焦点を当て、その後、それらに該当しない資産に焦点を当てる。 **注：**OT境界外への通信を阻止する有効なサイバーセキュリティ管理策（例：ファイアウォール）がない場合、ポート／サービスに関しては、すべての資産に焦点を当てることになる。	高
ユーザーアカウント	どのユーザーアカウントが最も頻繁に利用されると予想されるか、またはその資産に多くの異なるユーザがアクセスすると予想されるかを把握する上で役立つ。	高
バックアップの頻度／種類	バックアップがどのくらいの頻度で実行されるか（例：毎日、毎週、毎月）および使用される方法（例：完全バックアップ、増分バックアップ、差分バックアップ）を示す。	中
ベースラインイメージ	OSのインストールの基になった特定の正常なイメージが存在するかどうかを把握するのに役立ち、インシデント後の復旧を支援する。	中
部署／所有者	その資産を所有する者、またはその資産に責任を負う者を把握するのに役立つ。	中

資産インベントリの項目	属性の利点	優先度
販売業者	資産の出所（製造業者とは限らない）を把握するのに役立つ。	中
ファームウェア／ソフトウェアのバージョン	該当する場合は、既知の脆弱性を特定するのに役立つ。	中
OSのバージョン	該当する場合は、既知の脆弱性を特定するのに役立つ。	中
物理または仮想	資産が物理であるか、または仮想であるかについての情報を提供する。	中
仮想ローカルエリアネットワーク（VLAN）	資産のネットワーク構造を可視化する。	中
ウイルス対策（AV）／エンドポイント保護	資産が悪意ある活動から自らを防御するケイパビリティに関する詳細を提供する。	低
製造年月日	陳腐化を判断するのに役立つ。	低
ハイパーバイザー（該当する場合は）	仮想マシン（VM）を実行しているハイパーバイザーの種類に関する文脈を提供する。	低
ローカルタイムゾーン	タイムラインが関係するユーザ行動分析を行う際に役立つ。	低
ハイパーバイザー内の位置（該当する場合）	仮想マシン（VM）がハイパーバイザー内のどこに存在するかに関する文脈を提供する。	低
ネットワーク監視	資産への通信が、潜在的に悪意のある通信を検知するためにどの程度適切に監視されているかに関する情報を提供する。	低
注記／説明	資産に関する追加情報、その使用方法、過去に発生した問題などを提供する。	低
主な通信方法	攻撃対象領域を限定し、インシデントがローカル、リモート、またはネットワーク全体（例：有線、無線、携帯電話、マイクロ波／無線周波数（RF）、衛星）のいずれに該当するかをアセスメントするのに役立ち、通信プロトコルに関連している。	低
シリアル番号	一意の識別子。ベンダーのパッチ／サポートへのアクセスを確認するために必要となる。	低

資産インベントリの項目	属性の利点	優先度
時刻ソース	外部の時刻ソースの中断およびそれに伴うずれは、重大なインパクトを及ぼす可能性があるため、資産がどのように動作を同期させているか（例：ネットワークタイムプロトコル（NTP）、GPS、原子時計、ローカルクロック）を明確にする。	低

附属書B：石油・ガス組織向け分類体系

CISAは、石油・天然ガス下位分野のワーキングセッション参加者とともに、組織が独自のOT分類体系を作成するために必要なステップを識別するための仮想演習を実施した。この演習は仮想形式で実施されたため、CISAは物理的なサイト、コンポーネントの詳細または資産の属性、依存関係、もしくはデータフローに関する直接的な知識を必要とする活動は実施しなかった。

作成機関は、石油・天然ガス下位分野の組織に対し、独自の分類体系を作成するための一例として、この分類体系を使用するよう推奨している。

演習のステップ

1. **資産を識別する。**
   a. CISAは、迅速なデータ収集の演習を通じて、石油および天然ガス資産の概念的なリストを作成した。CISAは物理的な検査を実施できなかったため、参加者と共に主要なOTプロセス領域の識別から開始した。
      i. 安全システム
      ii. 管理／エンジニアリング
      iii. プロセス制御および監視
      iv. 環境システム
      v. 通信システム
      vi. ネットワーク機器
      vii. サイバーフィジカルセキュリティ
   b. 主要なプロセス領域を識別した後、CISAは各主要プロセス領域について、表2に示す概念的な資産を識別した（このリストは網羅的なものではなく、関連するすべての資産を網羅しているとは限らない）。

表2：OTプロセス領域別の石油・天然ガス下位分野組織の概念的な資産リスト

安全	管理／エンジニアリング	プロセス制御および監視	環境	通信	ネットワーク機器	サイバーフィジカルセキュリティ
緊急停止	一時的に接続されたデバイス（すなわち、ノートパソコン、リムーバブルメディア）	SCADA	スタック監視	有線	ネットワークスイッチ	IDおよびアクセス管理
火災およびガスシステム	統合データ管理システム	分散制御システム（DCS）	継続的な環境監視	マイクロ波バックホール	ファイアウォール	検知および監視システム

安全	管理／エンジニアリング	プロセス制御および監視	環境	通信	ネットワーク機器	サイバーフィジカルセキュリティ
コントローラ／安全計装システム	リモートアクセス（ジャンプサーバー）	PLC	漏洩検知	産業用IoT（IIoT）ネットワーク	インフラ監視（稼働時間、パフォーマンス、障害状況）	ウイルス対策／パッチ適用
イベントのシーケンス	バックアップおよび復旧	高度なプロセス制御	ヒートトレーシング	セルラーモデム	無線アクセスポイント	脆弱性スキャン
電気安全／負荷遮断	エンジニアリング保守ネットワーク	ヒストリアン	ビルマネジメントシステム（BMS）	双方向無線ネットワーク	メディアコンバータ	エンドポイント検知
ダイナミックポジショニング	仮想化／コンテナ／オーケストレーション	サードパーティ製パッケージ（例：コンプレッサー、タービン制御、バーナー、パッケージボイラー）	電力管理システム	光ファイバーネットワーク	データダイオード	物理アクセス制御システム

2. **資産に重要度を付ける。**
   a. CISAは、セキュリティ上の考慮事項に基づき、3つの重要度分類を作成した。
      i. 重要度「高」の資産には、ネットワークのセグメンテーションおよび役割ベースのアクセス制御など、最も厳格なセキュリティ対策が望ましい。
      ii. 重要度「中」の資産には、信頼性を確保するために、堅牢な監視および定期的な更新が望ましい。
      iii. 重要度「低」の資産には、基本的なセキュリティ対策が望ましい。これらは、網羅性のためにインベントリに含まれる。
   b. CISAは、以前に識別した主要なプロセス領域（**表2**）を機能ごとに細分化した。

3. **資産を重要度別にグループ化する。**

   a. CISAは、これらの*機能*を類似するカテゴリーにグループ化した（すなわち、ゾーン。CISAは、ゾーンを重要度別にグループ化した）。その結果、**表3**から**表5**に示すような資産分類体系が得られた。

表3：重要度「高」の資産

一次生産システム	安全システム	制御システム	電力システム
掘削リグ	緊急停止システム（ESD）	DCS	バックアップ発電機
坑口装置	火災およびガス検知システム	重要プロセス用PLC	無停電電源装置（UPS）
海底機器	噴出防止装置（BOP）		

表4：重要度「中」の資産

処理機器	監視システム	通信システム	ネットワーク機器
分離器（石油、ガス、水）	状態監視用センサー（振動、温度、圧力）	SCADAシステム	プロセス制御ネットワーク用スイッチおよびルーター
コンプレッサー	データヒストリアン	遠隔端末装置（RTU）	
熱交換器			

表5：重要度「低」の資産

補助システム	重要度の低い監視	周辺デバイス
暖房・換気・空調（HVAC）システム	環境監視（例：排出量の追跡）	オペレータワークステーション
照明システム	重要度の低いデータログ記録	重要度の低いヒューマン・マシン・インタフェース（HMI）

4. **次のステップ。**

   a. CISAは、「資産およびその通信経路の整理」、「構造および関係の整理」ならびに「検証および可視化」のステップを完了しなかった。これらは、識別された資産および展開済みの通信経路ならびにプロセスの依存関係に関する知識を必要とするためである。

実際のインベントリでこれらの次のステップを完了することで、石油・天然ガス下位分野の組織は、資産のゾーン、コンジットおよびカテゴリー、ならびに資産間の関係と依存関係を示した分類体系を作成できるようになる。これにより、自社のOT環境を正確に表す分類体系を作成し、インベントリの完成に役立てることが可能となる。

附属書C：電力組織向け分類体系

CISAは、エネルギー分野の電力組織からのワーキングセッション参加者と共に、組織が独自のOT分類体系を作成するために必要なステップを識別するために、仮想形式の演習を実施した。この演習は仮想形式であったため、CISAは物理的なサイト、コンポーネントの詳細、あるいは資産の属性、依存関係、データフローに関する直接的な知識を必要とする作業は行わなかった。

作成機関は、エネルギー分野の組織に対し、独自の分類体系を作成する際の事例の一つとして、この分類体系を使用するよう推奨している。

演習のステップ

1. **資産を識別する。**
    a. CISAは、迅速なデータ収集の演習を通じて、電力組織の資産の概念的なリストを作成した。CISAは物理的な検査を実施できなかったため、参加者と共に主要なOTプロセス領域の識別から開始した。
        i. DMZ
        ii. 通信システム
        iii. 発電
        iv. 送電および配電
        v. 物理アクセス制御、電子アクセス制御、または監視システム
        vi. エネルギーマネジメントシステム（EMS）
        vii. 分散型エネルギー源（DER）蓄電
        viii. エネルギー
    b. 主要なプロセス領域を識別した後、CISAは各主要プロセス領域について、**表6**に示す概念的な資産を識別した（このリストは網羅的なものではなく、関連するすべての資産を網羅しているとは限らない）。

表6：OTプロセス領域別の電力組織の概念的な資産リスト

DMZ	通信	発電	送電・配電	物理アクセス制御、電子アクセス制御、または監視システム	エネルギーマネジメントシステム（EMS）	分散型エネルギー源（DER）	エネルギー貯蔵
ファイアウォール	デジタル・アナログ変換器（DAC）	HMI	保護制御（リレー）	バッジリーダー／スマートキー	状態監視（すなわち、デジタル故障記録）	インバータとの通信	電力制御システム（すなわち、バッテリー管理システム）
アプリケーションサーバー	マイクロ波	PLC	HMI	カメラ	集中型是正措置スキーム（CRAS）	ハイブリッドインバータ	監視
サイバー監視ツール	衛星	エンジニアリングワークステーション	エンジニアリングワークステーション	役割ベースのアクセス制御	故障点特定・隔離・サービス復旧（FLISR）	電力制御システム（分散型エネルギーリソース管理システム）	保守
リモートアクセスサーバー	光ファイバー	ローカルエリアネットワーク（施設の築年数による）	RTU／PLC	モーション検知器	フロントエンドプロセッサ	バイオマス発電機	ポンプ／水力
侵入検知・防止サービス	ルーター／スイッチャー	タービン制御システム	スマートメーター	侵入検知システム	アラームおよび事象通知	太陽光発電（PV）システム	熱システム

DMZ	通信	発電	送電・配電	物理アクセス制御、電子アクセス制御、または監視システム	エネルギーマネジメントシステム（EMS）	分散型エネルギー源（DER）	エネルギー貯蔵
データヒストリアン	セルラーモデム	再生可能エネルギー	電力線搬送通信システム	制御アクセスポイント	フェーザー測定装置	燃料電池	圧縮空気

2. **資産に重要度を付ける。**
   a. CISAは、セキュリティ上の考慮事項に基づき、3つの重要度分類を作成した。
      i. 重要度「高」の資産には、ネットワークのセグメンテーションおよび役割ベースのアクセス制御など、最も厳格なセキュリティ対策が望ましい。
      ii. 重要度「中」の資産には、信頼性を確保するために、堅牢な監視および定期的な更新が望ましい。
      iii. 重要度「低」の資産には、基本的なセキュリティ対策が望ましい。これらは、網羅性のためにインベントリに含まれる。
   b. CISAは、以前に識別した主要なプロセス領域（**表6**）を機能ごとに細分化した。
3. **資産を重要度別にグループ化する。**
   a. CISAは、これらの機能を類似するカテゴリーにグループ化した（すなわち、ゾーン。CISAは、ゾーンを重要度別にグループ化した）。その結果、**表6**から**表9**に示すような資産分類体系が得られた。

表 7：重要度「高」の資産

主要設備	保護システム	制御システム	電源システム
電力変圧器	保護リレー（過電流／低電流）、距離型（インピーダンス、リアクタンス）、差動型（電流、電圧）	DCS	バックアップ発電機
遮断器	故障検知および隔離メカニズム	重要な機能を管理するPLC	重要な設備用UPS
開閉装置	電圧調整器	SCADAシステム	

一次機器	保護システム	制御システム	電源システム
母線（Busbars）			

表8：重要度「中」の資産

監視・計測デバイス	通信システム	環境制御システム
電流・電圧センサー	RTU	変圧器または制御室用冷却システム
エネルギーおよび電力品質の計測デバイス	ゲートウェイ	暖房・換気・空調（HVAC）
運用上の知見のためのデータヒストリアン	ネットワーク機器（スイッチ、ルーター）	

表9：重要度「低」の資産

施設支援システム	周辺デバイスおよび非重要デバイス	重要度の低い監視
屋内および屋外施設の照明システム	二次的または緊急性の低いシステム用のHMI	周囲温度センサー
建物のセキュリティシステム（非重要ゾーン）	管理タスクに使用されるオペレーター用ワークステーション	軽微な運用閾値用の警報システム

4. **次のステップ。**
    a. CISAは、「資産およびその通信経路の整理」、「構造および関係の整理」ならびに「検証および可視化」のステップを完了しなかった。これらは、識別された資産および展開済みの通信経路ならびにプロセスの依存関係に関する知識を必要とするためである。実際のインベントリでこれらの次のステップを完了することで、石油・天然ガス下位分野の組織は、資産のゾーン、コンジットおよびカテゴリー、ならびに資産間の関係と依存関係を示した分類体系を作成できるようになる。これにより、自社のOT環境を正確に表す分類体系を作成し、インベントリの完成に役立てることが可能となる。

附属書D：上下水道

CISAは、上下水道分野の組織からのワーキングセッション参加者と共に、組織が独自のOT分類体系を作成するために必要なステップを識別するために、仮想形式の演習を実施した。この演習は仮想形式であったため、CISAは物理的なサイト、コンポーネントの詳細、あるいは資産の属性、依存関係、データフローに関する直接的な知識を必要とする作業は行わなかった。

作成機関は、上下水道分野の組織に対し、独自の分類体系を作成する際の事例の一つとして、この分類体系を使用するよう推奨している。

演習のステップ

1. **資産を識別する。**
   a. CISAは、迅速なデータ収集の演習を通じて、上下水道資産の概念的なリストを作成した。CISAは物理的な検査を実施できなかったため、参加者と共に主要なOTプロセス領域の識別から開始した。
      i. 収集
      ii. 水処理
      iii. 配水
      iv. 再利用水
      v. データ管理 – 事業体統合サポートへの拡張
      vi. 下水処理
      vii. 通信インフラ
   b. 主要なプロセス領域を識別した後、CISAは各主要プロセス領域について、**表10**に示す概念的な資産を識別した（このリストは網羅的なものではなく、関連するすべての資産を網羅しているとは限らない）。

表10：上下水道の機能ベースのOT分類体系

収集	水処理	配水	再利用水	データ管理 - 事業体統合サポートへの拡張	下水処理	通信インフラ
下水流量計測ピット	水質（pH、監視システム）	圧力監視センサー	ポンプ場	可視化および報告ツール	ポンプ場	光ファイバー
下水ポンプ場	プロセス制御（PLC／RTU）	遠隔バルブシステム	減圧弁ピット	ビジネスインテリジェンス分析	生物処理	産業用イーサネット

収集	水処理	配水	再利用水	データ管理 - 事業体統合サポートへの拡張	下水処理	通信インフラ
測定（流量計）	薬液注入	バックアップ電源管理	品質	コンプライアンス	固形物処理	産業用無線
タンク水位センサー	環境	計測器／遠隔計測	計測	データベース／データレイク	高度処理	セルラー
水質センサー	温度変換器	IoTセンサー	曝気槽	転送中のデータを保護するためのサイバーセキュリティ対策	一次沈殿槽	免許制および免許不要の無線ネットワーク
圧力トランスデューサー	栄養塩除去システム	減圧弁	処理水貯水槽の水位	データ通信／ポーリングソフトウェア（OPC UA、MQTT、Modbus）	汚泥脱水システム	マイクロ波バックホール

2. **資産に重要度を付ける。**
   a. CISAは、セキュリティ上の考慮事項に基づき、3つの重要度分類を策定した。
      i. 重要度「高」の資産には、ネットワークのセグメンテーションおよび役割ベースのアクセス制御など、最も厳格なセキュリティ対策が望ましい。
      ii. 重要度「中」の資産には、信頼性を確保するために、堅牢な監視および定期的な更新が望ましい。
      iii. 重要度「低」の資産には、基本的なセキュリティ対策が望ましい。これらは、網羅性のためにインベントリに含まれる。

b. CISAは、以前に識別した主要なプロセス領域（**表6**）を機能ごとに細分化した。

3. **資産を重要度別にグループ化する。**

a. CISAは、これらの機能を類似するカテゴリーにグループ化した（すなわち、ゾーン。CISAは、ゾーンを重要度別にグループ化した）。その結果、**表11**から**表13**に示すような資産分類体系が得られた。

表 11：重要度「高」の資産

一次処理システム	二次処理システム	安全・環境システム	制御システム	電力システム
ポンプ（例：取水、排水、高圧）	曝気システム	緊急停止システム	SCADAシステム	バックアップ発電機
スクリーン、沈殿槽、および砂除去システム	生物処理槽	pH制御または消毒のための薬品注入システム	中核プロセス用DCS	UPS
		流出封じ込めシステム	OT通信インフラ	

表12：重要度「中」の資産

水質監視	通信システム	ネットワーク機器	補助システム
濁度、塩素、または溶存酸素用のオンライン分析装置	RTU	ネットワークスイッチ	汚泥処理設備（例：ポンプ、遠心分離機）
サンプリングステーション	PLC	プロセス制御システム用ファイアウォール	重要度の低いポンプシステム（例：灌漑用水または設備用水）

表13：重要度「低」の資産

施設支援システム	周辺デバイス	重要度の低い監視
HVAC	重要度の低いプロセス用HMI	周囲温度、施設の水使用量、または一般的なアラーム用のセンサー
建物の照明システム	オペレーター用ワークステーション	

4. **次のステップ。**
    a. CISAは、「資産およびその通信経路の整理」、「構造および関係の整理」ならびに「検証および可視化」のステップを完了しなかった。これらは、識別された資産および展開済みの通信経路ならびにプロセスの依存関係に関する知識を必要とするためである。実際のインベントリでこれらの次のステップを完了することで、上下水道分野の組織は、資産のゾーン、コンジットおよびカテゴリー、ならびに資産間の関係と依存関係を示した分類体系を作成できるようになる。これにより、自社のOT環境を正確に表す分類体系を作成し、インベントリの完成に役立てることが可能となる。

参考文献

CVE.org。「Common Vulnerabilities and Exposures (CVE)」。2025年6月24日閲覧。https://www.cve.org/。

GitHub。「DINA-community/String-Sysiphos/Attributes of Data Model」。最終更新日：2025年8月2日。https://github.com/DINA-community/String-Sysiphos/blob/main/datamodel/datamodel_attributes.md。

アイダホ国立研究所（INL）。「Cyber-Informed Engineering.」。2025年6月24日閲覧。https://inl.gov/national-security/cie/。

国際自動制御学会（ISA）。*Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design, 2020*年。

MITRE。「CAPEC VIEW：産業用制御システム（ICS）パターン」。2025年6月27日閲覧。https://capec.mitre.org/data/definitions/703.html。

MITRE ATT&CK。「CAPEC VIEW: Industrial Control System (ICS) Patterns.」。2025年6月24日閲覧。https://attack.mitre.org/matrices/ics/。

Oasis。「Common Security Advisory Framework (CSAF).」。2025年8月8日閲覧。https://www.csaf.io/。