ICSCoE TLP: WHITE

制御システムにおける資産管理ガイドライン

資産管理の手引きとチェックリスト

2020 年 6 月

独立行政法人 情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム 3 期生

資産管理プロジェクト

目次

1 概要

1.1 はじめに

本ガイドラインは、制御システムにおけるサイバーセキュリティリスクに対応するために必要な資産管理についてまとめたものであり、資産管理、リスクアセスメント、リスクマネジントを担当する方々を対象としている。

1.2 本ガイドラインの背景

- IoT，デジタルトランスフォーメーション（DX）の普及や、生産性向上のため工場の製造現場が情報ネットワークに接続する機会が増加し、それに伴いサイバーセキュリティリスクも増加している。
- コストの削減や利便性の向上を達成する反面、増大するサイバーセキュリティリスクに対する備え（制御システムのセキュリティ対策）が課題になっている。
- サイバーセキュリティに起因する影響を最小限にするためにはリスクマネジメントの徹底が不可欠である。リスクマネジメントを実施するための ISO31000 で定義されている「組織の状況の確定」には、資産管理が必要になる。
- 効果的な制御システムのセキュリティ対策を実施するためには、リスクマネジメント、リスクアセスメントの各ガイドラインにおいても資産管理が必要（保護資産の明確化）とあるが、制御システムの資産管理について具体的な方法と課題に触れているガイドラインが殆どない。

【コラム】制御システムで資産管理を行うには課題がある

情報システムと異なり、制御システムでは稼働設備への可用性影響を考慮し資産管理製品の導入が難しい。そのため、情報システムと同様の管理手法で対応ができないといった課題が制御システム関係者へのアンケート結果から見えてきた。アンケートは ICSCoE※3 期生 69 名に制御システムの資産管理について調査した。インストールアプリやパッチ適用状況まで管理できている組織や、老朽化システムの更新計画も考慮した構成管理を展開できている組織もある一方、多くの組織が資産管理に課題を持っていることがわかった。図 1 は 69 名のうち、「制御システムを所持かつ資産管理をしている」19 組織の資産管理の課題をまとめたものになる。

※ICSCoE 産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）
https://www.ipa.go.jp/icscoe/index.html

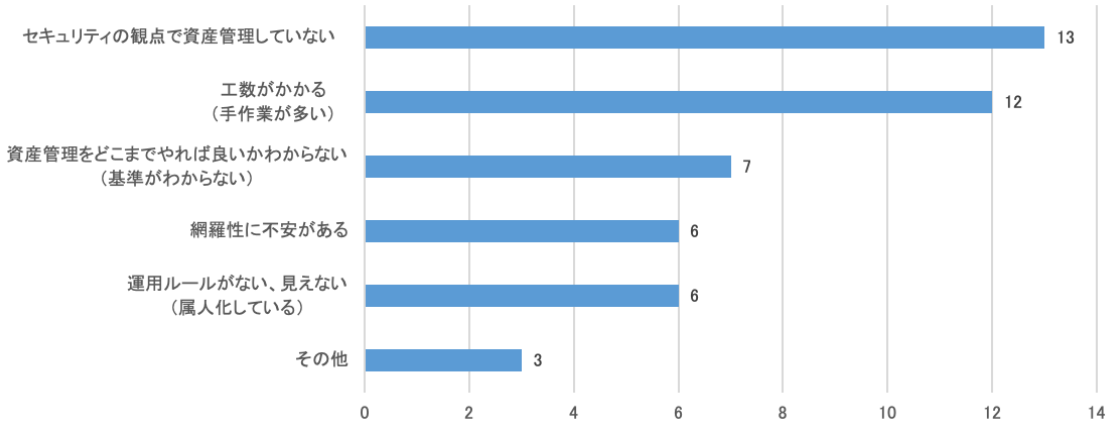

図 1 制御システム資産管理の課題

セキュリティ観点で資産管理ができていない、手作業が多く工数が掛かる、資産情報をどこまで収集管理すれば良いかわからないという課題が多い。

図 2 の資産管理手法のアンケート結果から、紙・エクセルによる手作業での台帳管理が多いことも分かり、工数がかかる要因と考えられる。

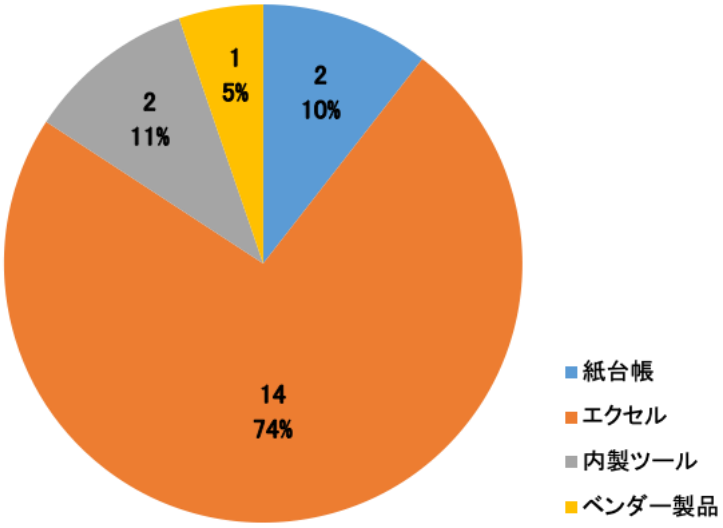

図 2 制御システムの資産管理手法

2　本ガイドラインの目的

上記のような背景を受け、以下を目的としたガイドラインを作成した。

- 制御システム関係者が制御システムの資産管理に関する理解を深め、その取り組みが促進されること
- 制御システムの資産管理を具体的に実施するための手引きを示すこと
- 制御システムの資産管理のチェックリスト及び成熟度モデルを示し、ギャップ分析の一助となること

本ガイドラインを活用することで、制御システムの資産管理に取り組む組織が増加し、セキュリティレベルの向上につながることを期待する。

なお、本ガイドラインを作成するにあたって IPA※の「制御システムのセキュリティリスク分析ガイド　第２版」（以後、IPA 分析ガイドと略する）を参考かつ引用している。

※IPA　独立行政法人情報処理推進機構（Information-technology Promotion Agency）
https://www.ipa.go.jp/about/ipajoho/gaiyo.html

3 本ガイドラインの活用方法

3.1 対象者

本ガイドラインで想定される対象者には、次の者が含まれる。ただし、これらに限定されない。

- 制御システムにおいてリスクマネジメントを行うもの
- 制御システムにおいてリスクアセスメントを行うもの
- 制御システムにおいて資産管理を行うもの

3.2 本ガイドラインの効果

本ガイドラインを活用することで、制御システムにおける資産管理の成熟度を向上させ、サイバーセキュリティリスクの低減と、より適切な管理を実現することである。

- 資産管理を未実施の場合は、実施方法を提供し、次工程（リスクアセスメント等）へ繋げられるようにする
- 資産管理をセキュリティの観点で実施していない場合は、適切な手引きを示し、セキュリティ対策に繋げられるようにする
- 資産管理を手作業で実施している場合には、自動化の方法を提供し、資産管理の効率化を支援する

3.3 方法論

本ガイドライン作成にあたって従った方法論は、以下の５つのタスクからなる。

タスク１：資産管理の調査とプロジェクト範囲の決定

各種ガイドライン調査、アンケート調査を踏まえて、制御システムの資産管理に考慮される情報を検討し、プロジェクトの範囲を決定した。

タスク２：項目抽出

タスク１のステップで検討した情報をもとに、制御システムの資産管理を効果的にするための項目を精査した。

タスク３：ガイドライン本文の作成

タスク２までのステップでまとめた情報を更にブラッシュアップし、ガイドラインとして作成した。

タスク４：自動化ツールの開発・検証および資産情報収集可能な製品の検証

制御システムの資産管理における成熟度を向上させる上で、自動化ツールの開発を行い、資産情報の収集・台帳作成/更新の自動化の有効具合を検証した。また資産情報収集可能な製品を検証し、商用製品を導入する上で検討すべき項目を調査した。

タスク５：レビューと検証

セキュリティ専門家とガイドラインを共有し、コメントやフィードバックを得て、このガイドラインの最終版が作成された。

3.4 本書の構成

本ガイドラインは資産管理を未実施の場合、各章毎に読んでいくことで理解しやすいように構成している。資産管理を既に実施している場合、本章以降は以下の構成を参考に必要な章を読み、効率的に活用してもらいたい。

資産管理概説（4 章）

制御システムにおける資産管理の必要性や位置づけを概説し、セキュリティ対策における資産管理を理解する。

脅威情報と資産情報（5 章、6 章、7 章、8 章）

本ガイドラインの対象を定義し（5 章）、制御システムにおける脅威（6 章）と脅威を把握するために収集すべき資産情報を示し（7 章）、脅威との関連付けを実施する事で脅威を迅速に検知する資産管理を理解する（8 章）。

資産情報の収集方法（9 章、10 章、11 章）

資産情報の収集方法と考え方を説明し（9 章）、自動化ツール開発と自動化の有効具合の検証を通してツール紹介する（10 章）。資産情報を収集できる製品の検証結果を述べる（11 章）。ここでは具体的な収集方法について理解する。

自組織の資産管理レベルの評価と向上（12 章、13 章）

セキュリティ対策の向上を目的に資産管理レベルを評価する成熟度モデルの定義（12 章）とチェックリスト（13 章）を紹介する。

資産管理の手引き（14 章）

制御システムにおける資産管理の手引きを述べる。

4　セキュリティ対策における資産管理の位置付け

4.1 制御システムにおける資産管理の必要性

従来の制御システムはインターネットなどの外部の情報ネットワークから隔離されていた。しかし生産性向上のため、IoT 機器や Web カメラ等が気軽に導入できるといった環境変化により、制御システムが情報ネットワークに接続する機会が増加している。その結果、制御システムにおいても情報ネットワークと同様に「不正端末によるサイバー攻撃」「脆弱な端末を狙ったサイバー攻撃」といったサイバーセキュリティ上の懸念が高まり、セキュリティを意識した資産管理が必要となっている。

4.2 資産管理はセキュリティ対策の土台

ISO31000 リスクマネジメントプロセス（図 3 参照）ではリスクアセスメントの前段として、「組織の状況の確定」がある。その中で内部状況の「情報システム、情報の流れ及び意識決定プロセス」の整理が必要であり、この整理を素早く、適切に実施することが、リスクアセスメントの質向上につながり、さらにはリスクマネジメントの質向上につながるため、最終的にはセキュリティ対策につながると考えている。

資産管理とは、まさにこの整理を素早く、適切に意思決定するための土台である。

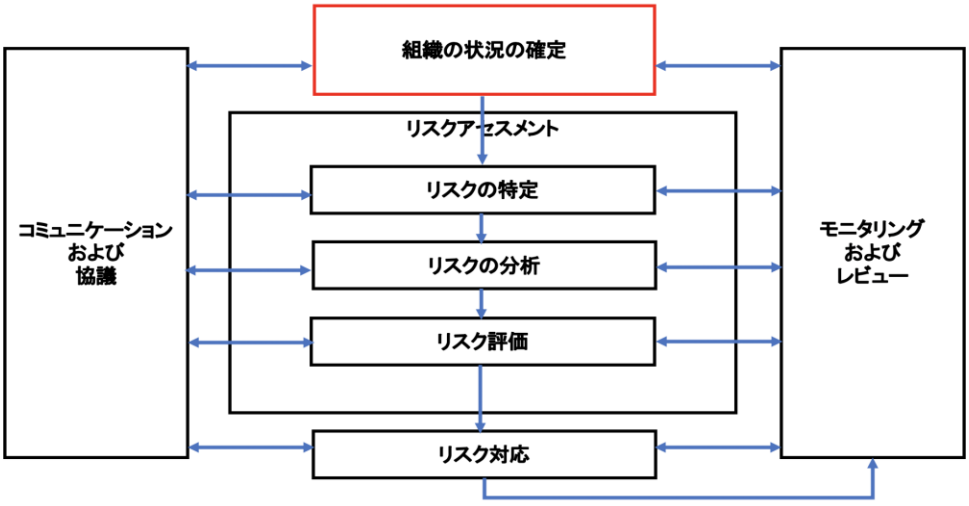

図 3　ISO31000 リスクマネジメントプロセス

他にも IEC62443 制御システムセキュリティ標準や NIST※1、NISC※2 などが公開する各種ガイドラインにおいてリスクアセスメントの実施が求められている。よってリスクアセスメントの質を上げるための資産管理が大切である。

資産管理（現状把握）ができていないと異常に気づけないため、常に最新情報に更新するべきである。

実態の把握と対策を検討する場合は、数ある分析手法の中でも IPA 分析ガイドの「詳細リスク分析」が適している。さらに詳細リスク分析の中に「資産ベース手法」があり、資産に対する脅威を網羅的に洗い出すことができ、リスク分析を円滑に着手することができる。

※1 NIST 米国標準技術研究所（National Institute of Standards and Technology）
https://www.nist.gov/

※2 NISC 内閣サイバーセキュリティセンター
（National center of Incident readiness and Strategy for Cybersecurity）
https://www.nisc.go.jp/

4.3 セーフティとセキュリティにおける脅威の重要性の違い

制御システムは、セキュリティ要件ではなく、故障対策に基づいたエンジニアリング要件を満たす様に設計されている。そのためセーフティな制御システムでは、機器の故障対策として可用性を重視していた。老朽化した機器も冗長機能を持つ事でセーフティにおける脅威に対応していた。

ただし、セキュリティ視点では考え方を見直す必要がある。老朽化によりレガシーなシステムになる事で、セキュリティの脆弱性を持てばたちまちに危険な状態となる。

例えば、セーフティ視点では HMI(Human Machine Interface)を複数台設置することで可用性が高まり、脅威の小さい資産とみなせる。しかし、セキュリティ視点となると Windows OS の HMI は、脆弱性を持つものであり、脅威の大きい資産とみなされる。

セキュリティ対策における資産管理では、セーフティとの違いも考慮することが大切である。

5 資産管理対象の範囲

本ガイドラインにおいて資産管理の対象としている範囲を下記に定義する。資産管理対象の主な制御システムの特徴を表 1 に示す。

- 制御システムにおける制御ネットワーク（情報側）の機器、制御ネットワーク（フィールド側）の機器およびフィールドネットワークのコントローラまでを対象とする（図 4 参照）
- コントローラ配下のフィールド機器（センサー、アクチュエータ等）は機器固有の安全対策という視点から設備管理としての資産管理を適用することを想定し、本ガイドラインでは対象外としている
- DMZ、情報ネットワークについては（各組織で業務所掌の考え方は異なるが）、一般的には情報ネットワークの資産管理を適用することを想定し、本ガイドラインでは対象外としている

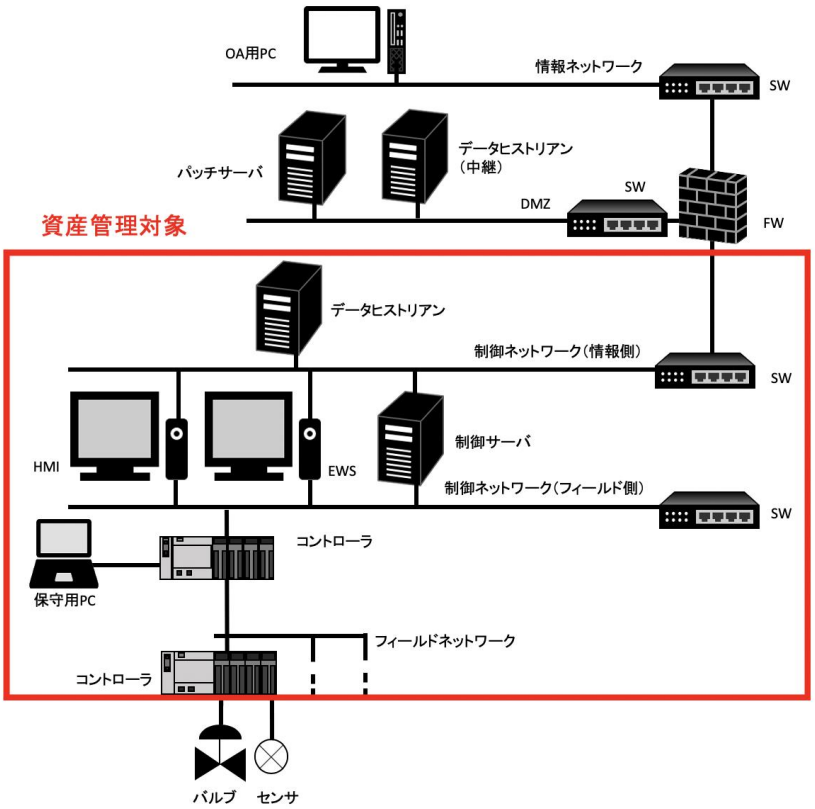

図 4　資産管理対象

表 1　資産管理における制御システムの定義と特徴

名　称	説　明
PLC (Programmable Logic Controller)	制御システムにおける制御を自動化するための専用の産業用コンピュータ。 PLC 配下に接続されるフィールド機器を制御し、独自のタッチパネル表示器で監視操作も可能。 オープンな通信プロトコルを採用し、HMI 等の接続の組み合わせは多様。 PLC 単一の小規模システムや、DCS、SCADA のシステム内のローカルコントローラとして接続される事が多い。 複数メーカーとの接続が多くなるため、制御システムオーナーが主体的にセキュリティ対策を管理する必要がある。
DCS (Distributed Control System)	制御プロセスについての情報、すなわち管理ロジックを単一の中央処理装置に頼るのではなく、分散した装置をネットワークで接続して制御するシステム。システムとして HMI、コントローラを分散して持ち、メーカー独自プロトコルで接続される。 制御ネットワーク（フィールド側）は DCS メーカーが一式のシステムで保証するため、汎用ソフトウェア等の導入は困難である。制御システムオーナーで実施できる対策は外部接続の境界対策とエンドポイントの運用管理であり、オーナーのみでのセキュリティ対策の実施には高いハードルがある。 また、システム管理はメーカー固有が多いため、汎用資産管理ツールを使用することは難しい。 よって、本ガイドラインで定義する資産情報については各々のシステム管理画面やネットワーク構成図を参照する必要がある。
SCADA (Supervisory Control and Data Acquisition)	産業用資産及びプロセスからのデータ収集、それらの可視化、監視及び制御管理に使用されるシステム。遠隔地のステーションをコントロールセンターで監視する等、大規模で遠隔に接続される。 専用コントローラを持つことは殆どなく、オープンな通信プロトコルで PLC、DCS と接続され、組み合わせは多様。 複数メーカーのシステム（PLC、DCS 等）が接続され、大規模、遠隔になる環境であり、制御システムオーナーが主体的にセキュリティ対策を管理する必要がある。
IIoT (Industrial Internet of Things)	センシング、アクチュエーティング、データの保存、及び処理などの様々な機能を持ち、ネットワークを介してデータを処理・交換する機器。 本ガイドラインでは IIoT ネットワークは制御ネットワークとは隔離して設計することを推奨し、IIoT エンド機器の資産管理については対象外としている。 一方で、IIoT の通信経路が従来の制御ネットワークと直接接続するゲートウェイ（無線アクセスポイント含む）等については、サイバーセキュリティの観点から管理する必要があり、本ガイドラインの対象とする。

【コラム】DCS システムにおける資産管理とメーカー保証

表 1 で特徴を示すように、DCS システムにおける資産管理はネットワーク毎に留意する必要がある。

制御ネットワーク（情報側）については、汎用資産管理ツールによる検知、管理も可能であり、DCS メーカーによるサイバーセキュリティ対策商品・サービスも提供されているので、セキュリティ対策に検討すると良い。

ただし、DCS システム内の機器に汎用資産管理ツールのエージェントや管理ソフトウェアをインストールする際には、それらソフトウェアが DCS の動作に影響する場合があるので、メーカー保証を考慮する必要がある。

また、制御ネットワーク（フィールド側）についてはメーカー固有プロトコルが使われる場合は、汎用資産管理ツールによる検知、管理が困難である。また上記と同様にメーカー保証、及び制御システム自体への影響も無視できないため、DCS メーカーと協議の上セキュリティ対策を進めるべきである。

6　制御システムにおける脅威とは

攻撃手法の観点で分類した脅威を、以下「脅威(攻撃手法)」と示す。脅威(攻撃手法)は、資産種別（資産種別の詳細については 7 章を参照）によって異なる。情報系資産と制御系資産に対して想定される脅威(攻撃手法)を表 2 に、ネットワーク資産に対して想定される脅威(攻撃手法)を表 3 に示す。

資産管理においてはこれらの脅威に対応できるように資産の情報を収集する必要がある。なお本項目は IPA 分析ガイドを参考に作成しており、新たな脅威(攻撃手法)が発生した場合や、組織特有の脅威(攻撃手法)が存在する場合は、項目について再検討が必要となる。また図 5 は IPA 分析ガイドに掲載されている典型的な攻撃手順の表現例になる。表 2,3 と併せて確認することで脅威（攻撃手法）の理解に役立てていただきたい。

表 2 情報系資産と制御系資産に対する脅威（攻撃手法）(1/2)

項番	脅威 （攻撃手法）	説明	具体例
1	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用 ・設定不備（※1）の悪用
2	物理的侵入	制御システムが設置された区域・箇所へ侵入し、攻撃を実行する。	・入出制限区域（※2）への不正侵入 ・ラック、設置箱の不正開放
3	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用
4	過失操作	内部関係者の過失操作を誘発、攻撃の代わりとする。 正規の媒体・機器を悪用し、攻撃に相当する行為を実行させる。	・持ち込む正規媒体のマルウェア感染 ・メールの不審な添付ファイル開封・実行 （マルウェア感染）
5	不正媒体 機器接続	不正に持ち込んだ媒体・機器（※3）を接続し、攻撃を実行する。	・不正媒体の接続
6	プロセス不正実行	機器上の正規プログラム・コマンド・サービスを、不正に実行・起動する。	・意図しない動作の実行

表 2 情報系資産と制御系資産に対する脅威（攻撃手法）(2/2)

項番	脅威 （攻撃手法）	説明	具体例
7	マルウェア感染	機器にマルウェア（不正プログラム）を感染させる。	・マルウェアへ感染
8	情報窃取	機器に格納された情報を窃取する。	・格納情報（※4）の窃取
9	情報改ざん	機器に格納された情報を改ざんする。	・制御プログラム・パラメータの改ざん ・格納情報（※4）の改ざん
10	情報破壊	機器に格納された情報を破壊する。	・制御プログラム・パラメータの削除・暗号化 ・格納情報（※4）の暗号化
11	不正送信	機器を踏み台にして、他の機器へ不正な制御コマンド・データを送信する。	・制御コマンドの不正実行 ・制御プログラム・データの改ざん
12	機能停止	機器の機能を停止する。	・停止命令の不正実行
13	高負荷攻撃	機器能力以上の処理要求を行い、正常動作を妨害する。	・DoS 攻撃 ・DDoS 攻撃
14	窃盗	機器を窃盗する。	・機器の切り離し・持ち出し
15	窃盗・廃棄後の情報窃取	窃盗・廃棄された機器の保存情報が摂取される	・格納情報（※4）の流出

※１：不要プロセス動作や不要ポートの開放を指す。

※２：敷地内・計器室・サーバ室を指す。

※３：CD・DVD・USB 機器等を指す。

※４：ソフトウェア・認証情報・構成情報・暗号化機等を指す。

表 3 ネットワーク資産に対する脅威（攻撃手法）

項番	脅威 （攻撃手法）	説明	具体例
1	**経路遮断**	通信を遮断する。	・通信ケーブルの切断 ・ケーブル抜去
2	**通信輻輳**	容量以上の通信トラフィックを発生させ、輻輳状態とする。	・DoS 攻撃 ・DDoS 攻撃
3	**無線妨害**	無線通信を妨害する。	・妨害電波の送出
4	**盗聴**	ネットワーク上を流れる通信を盗聴する。	・ログイン情報の窃取 ・攻撃に備えた事前調査
5	**通信データ改ざん**	ネットワーク上を流れる情報を改ざんする。	・不正なプログラムに書換 ・表示データの改ざん
6	**不正機器接続**	ネットワーク上に不正機器を接続する。	・無許可 PC 等の不正接続 ・不正な無線アクセスポイントの設置

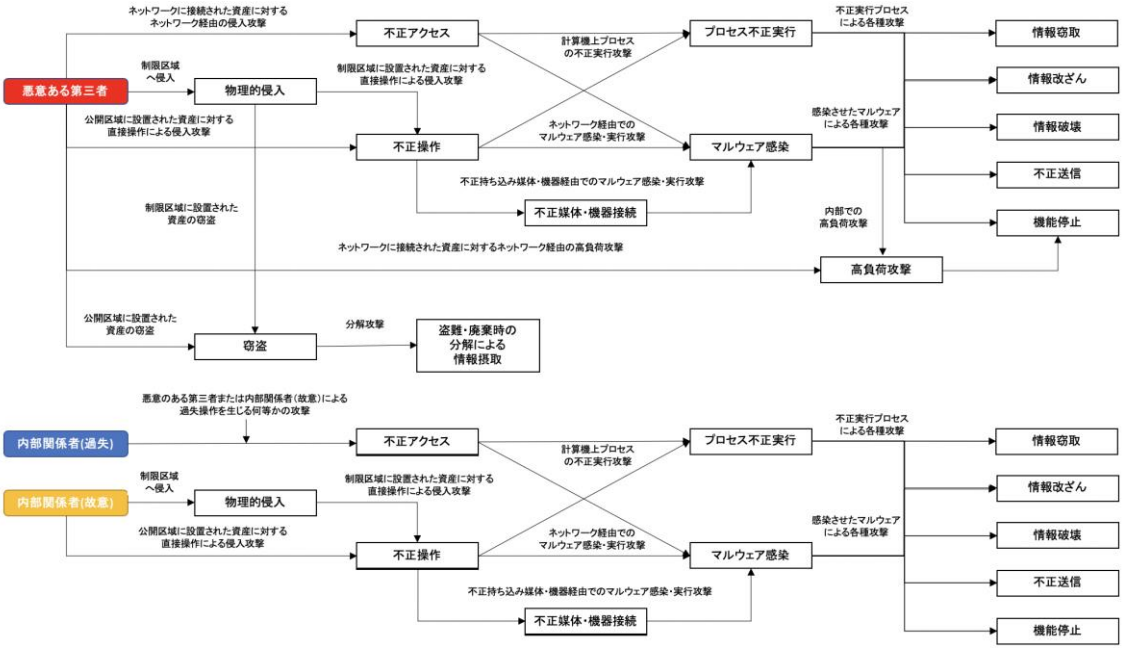

図 5　脅威（攻撃手法）を用いたサイバー攻撃の手順例

7 収集すべき資産情報について

制御システムにおける脅威に対応するための収集すべき資産情報を表 4、表 5 に示す。表 4 は IPA 分析ガイドで「資産に付帯される情報」にて定義されている資産情報であり、リスク分析等を行うための資産情報である。表 5 の資産情報は、表 4 と併せて本ガイドラインが収集を推奨する資産情報であり、本ガイドラインが推奨する資産管理を実現する。表 6 は本ガイドラインと IPA 分析ガイドの収集すべき資産情報の一覧を比較したものになる。

表 4 IPA 分析ガイド定義されている収集すべき資産情報（1/3）

情報の種類	意　味
資産名	資産の名前を記す。 資産名は役割や機能の他、IP アドレス、MAC アドレスで表すことがある。
資産種別	資産の種別を、以下の 3 種類に分類し記す。 • 情報系資産： サーバや PC（操作端末、監視端末等） • 制御系資産： 操作器を直接制御するコントローラ（PLC や DCS 等） • ネットワーク資産： ネットワーク回線やネットワーク装置。ネットワーク資産は、以下のいずれかに細分化する 　• 「通信制御機能あり」： 通信制御機能を有するネットワーク装置（ファイアウォールやスイッチ等）で構成されたネットワークに属する資産 　• 「通信制御機能なし」： 通信制御機能を持たないネットワーク装置（非インテリジェント HUB 等）で構成されたネットワークに属する資産
資産の持つ機能	資産種別＝「情報系資産」または「制御系資産」の場合、資産の持つ機能を記す。機能とは、その資産がシステムの中でどの様な動作をするかを明確にするための分類で、セキュリティ対策に密接に関連する。機能の分類は、 • 入出力 • データ保存 • （制御装置への）コマンド発行 • ゲート：ルータ、ファイアウォール（FW）、スイッチ（SW）等ネットワーク上でデータが通過する経路上に存在する機器 の 4 種類またはその組合せ（複数の機能を持つ機器）となる。セキュリティ対策との関連とは、例えば制御に利用するデータ保存機能を持つ資産では、その値が改ざんされると、システムに被害が生じる恐れがある。また、正規のコマンド発行機能を持つ資産から発行された不正なコマンドは、不正であると判断するのは難しく、誤動作を生じる恐れがある。
回線種類（ネットワーク）	資産種別＝「ネットワーク資産」の場合、機器間の通信が、WAN か LAN か、専用線かインターネット経由か、有線か無線かを記す。通信回線によっても、それぞれの特性に応じたセキュリティ対策が必要となる。

表 4 IPA 分析ガイド定義されている収集すべき資産情報（2/3）

情報の種類	意　味
設置場所	資産が設置されている場所を記す。設置場所により、物理的なセキュリティ対策状況（入室時の認証方法等）が異なる場合があるため、明確にする。
接続先ネットワーク	資産種別＝「情報系資産」または「制御系資産」の場合、資産がどの階層や機器にどの様に接続されているかを記す。
管理ポートの接続先	資産が持つ管理ポートの接続先を記す。資産種別＝「情報系資産」または「制御系資産」の場合、ファイアウォール機器等ではメンテナンスをネットワーク越しに行う様なケースがあり、通信ポートとは別の管理ポート経由で通信できる様になっている場合がある。
操作インタフェースの有無	キーボードやタッチパネルの様な操作を変更できるインタフェース（I/F）が接続されているかを記す。
USB ポート／通信 I/F の利用	資産の持つ USB ポートや通信ポートが、業務以外の目的で利用可能か否かを記す。
媒体・機器の接続の定常運用の有無	定常運用において、USB メモリやネットワーク機器等を資産に接続する機会があるか否かを記す。
無線機能の有無	無線通信機能やアクセスポイント機能（有線 LAN を無線 LAN に変換する機能）等を有するか否かを記す。
定常稼働、非定常稼働	定常的に稼働している資産か、必要な場合のみ稼働させる資産かを記す。非定常稼働機器を分析対象に含めるか除外するかは、最初の段階で方針を明確に決めておく。除外する場合は、最初から資産一覧表にまとめる作業は行わない。
データの種類と経路	資産種別＝「情報系資産」または「制御系資産」の場合、データ（コマンドを含む）の種類と経路（送信者、中継者、受信者）を記す。

表 4 IPA 分析ガイド定義されている収集すべき資産情報（3/3）

情報の種類	意味
構築ベンダー／機器メーカー	資産の提供元によって納入時やファームウエアアップデート等メンテナンスのポリシーが異なる場合があるので、個別に調べて記す。
OS の種類／バージョン	資産種別＝「情報系資産」または「制御系資産」の場合、OS の種類（ディストリビューションを含む）やバージョンによっては、既にサポートが終了してセキュリティパッチが提供されないケースがあるため、個々の資産の OS を調べて記す。
使用するプロトコル	資産が使用するプロトコルを記す。攻撃対象となりやすいプロトコルが使用されている場合もあり、対策が必要なケースがあるため、プロトコルも調査しておくことが望ましい。
セキュリティ対策	それぞれの資産が現在行っているセキュリティ対策を列挙して記す。

表 5　IPA 分析ガイドの資産情報と併せて収集すべき資産情報

情報の種類	意味
資産の重要度	資産が損なわれた場合の被害の大きさを記す。 資産自身の価値に加え、資産がサイバー攻撃を受けた時に想定される事業被害、事業継続性の影響を考慮し、リスクアセスメント時に定義する。リスクアセスメントの他、資産管理以降の工程で利用されるものであり、資産情報として台帳登録しておくことで作業の効率化を測ることができる。サイバー攻撃は重要度が低いところから攻撃を開始される場合があるため、リスクアセスメントを通じて、必要なセキュリティ対策実施を推奨する。
資産の担当者	資産の管理担当者を記す。 管理担当者が特定できることで資産が適切に管理され、なんらかのアクションが必要な場合に、組織が担当者に連絡を取れるようになる。
資産の責任者	資産の管理責任者を記す。 管理責任者が特定できることで資産が組織として責任を持って管理され、なんらかのアクションが必要な場合に、組織が責任者に連絡を取れるようになる。
IP アドレス	資産に設定されている IP アドレスを記す。資産の識別に利用することがある。
MAC アドレス	資産に設定されている MAC アドレスを記す。資産の識別に利用することがある。

表 6 収集すべき資産情報一覧の比較

資産情報の種類	収集すべき情報一覧	
	本ガイドライン	IPA 分析ガイド
資産名	●	●
資産種別	●	●
資産の持つ機能	●	●
回線種類（ネットワーク）	●	●
設置場所	●	●
接続先ネットワーク	●	●
管理ポートの接続先	●	●
操作インタフェースの有無	●	●
USB ポート／通信 I/F の利用	●	●
媒体・機器の接続の定常運用の有無	●	●
無線機能の有無	●	●
定常稼働、非定常稼働	●	●
データの種類と経路	●	●
構築ベンダー／機器メーカー	●	●
OS の種類／バージョン	●	●
使用するプロトコル	●	●
セキュリティ対策	●	●
資産の重要度	●	
資産の管理担当者	●	
資産の管理責任者	●	
IP アドレス	●	
MAC アドレス	●	

8 資産情報と脅威の関係性

IPA 分析ガイドを利用するにあたって制御システムにおける脅威（6 章）毎に、検知のため収集すべき資産情報（7 章）を関連付けた表を以下に示す。これらの対応に基づいてそれぞれの資産情報を適切に管理することで、潜在的な脅威や顕在化した脅威を迅速に検知することができる。なお、保有する制御システムに対しての新たな脅威を発見した場合は、改めて収集すべき資産情報との関連付けを管理する必要がある。

［凡例］

●　：脅威の検知に必要な情報

空白：脅威の検知には必要ではないが、次工程（リスクアセスメントなど）にて必要な情報

表 7　脅威と資産情報の関係性

脅威(攻撃手法)／資産	資産名	資産種別	資産の持つ機能	回線種類	設置場所	接続先ネットワーク	管理ポートの接続先	操作インターフェースの有無	USB ポート・操作 I/F の利用	媒体・機器の接続の定常運用の有無	無線機能の有無	定常稼働、非定常稼働	データの種類と経路	構築ベンダー、機器メーカー	OS の種類、バージョン	使用するプロトコル	セキュリティ対策	資産の重要度	資産の担当者	資産の責任者	IP アドレス	MAC アドレス
不正アクセス	●					●							●			●					●	●
物理的侵入	●				●																	
不正操作	●				●	●		●					●			●					●	●
過失操作	●					●							●			●					●	●
不正媒体・機器接続	●				●				●	●												
プロセス不正実行	●					●							●			●					●	●
マルウェア感染	●					●							●			●					●	●
情報窃取	●					●							●			●					●	●
情報改ざん	●					●							●			●					●	●
情報破壊	●					●							●			●					●	●
不正送信	●					●							●			●					●	●
機能停止	●					●							●			●					●	●
高負荷攻撃	●					●							●			●					●	●
窃盗	●				●																	
盗難・廃棄時の分解による情報窃取	●				●																	
経路遮断	●				●	●							●								●	●
通信輻輳	●					●					●(※1)		●			●					●	●
無線妨害	●				●(※2)	●					●		●								●	●
盗聴	●					●(※3)							●(※3)			●(※3)					●	●
通信データ改ざん	●					●							●			●					●	●
不正機器接続	●				●	●				●			●								●	●

※1 意図しない無線 AP 経由での通信輻輳の脅威に気づくことができる。

※2 運用拠点外部との境界近くにある機器が意図しない無線接続を試みられるという脅威に事前に気づくことができる。

※3 盗聴による攻撃が試行されたとしても、適切な経路の暗号化や重要データを通信路に流さないことで盗聴による攻撃の成立を防ぐことができる。攻撃方法によっては攻撃時の検知は困難だが、これらの情報を揃えておくことで脅威の存在するネットワークに事前に気づくことができる。

9 資産情報の収集方法について

制御システムにおいて、資産情報を収集する際に、制御システムとネットワークの種別に応じて適した収集方法がある。ついては制御システムの資産情報収集に対する考え方、ネットワークの資産情報収集に対する考え方、そして収集方法と取得可能な情報一覧について以下にまとめる。

表 8 制御システム毎の考え方

システム種別	考え方
SCADA	複数メーカーの DCS、PLC がネットワークに存在するため、制御システムオーナーが全て主体的に把握する必要がある。
DCS	制御ネットワーク（フィールド側）は DCS システム情報からの収集が一般的である。 制御ネットワーク（情報側）については、制御システムオーナー設置機器も含まれてくるため下記ネットワークごとの考えの制御ネットワーク（情報側）の管理は制御システムオーナーが主体的に実施する必要がある。 DCS については、DCS ベンダーへの相談が必須。DCS システムとして設置されているネットワーク機器はメーカーが保証し納入しているため、ミラーポート付きのスイッチ HUB に置き換え等は自主判断でしない。

表 9 ネットワーク毎の考え方

ネットワーク種別	考え方
情報ネットワーク	本ガイドラインの対象外
DMZ（DeMilitarized Zone）	本ガイドラインの対象外 なお、情報ネットワークと同様、基本的に Windows や Linux サーバのみであり、アクティブスキャン、エージェントによってシステム停止につながる可能性は低い。
制御ネットワーク（情報側）	基本的に Windows や Linux サーバのみであり、アクティブスキャン、エージェントによってシステム停止につながる可能性は低い（ネットワーク帯域圧迫によりデータ欠損など影響が生じる可能性がゼロではない）。 なお HMI 等、NIC（ネットワークインターフェースカード）2 枚構成で制御ネットワーク（フィールド側）に接続されている場合もあるため、間違って制御ネットワーク（フィールド側）に通信しないよう注意が必要である。 資産管理ソフト導入も可能だが、制御システムの保守期間は長く、サポート期限が終了した OS に対応されなくなる可能性もあるため、導入ソフトの保守期間を意識する必要がある。
制御ネットワーク（フィールド側）	アクティブスキャン、エージェントはネットワーク帯域圧迫、コントローラへの負荷によりシステム停止、データ欠損などにつながる可能性がある。パッシブスキャンだとシステムに影響を及ぼす可能性が低い。
フィールドネットワーク	アクティブスキャン、エージェントはネットワーク帯域圧迫、コントローラへの負荷によりシステム停止、データ欠損などにつながる可能性がある。IP アドレスを持たない機器もあるのでアクティブスキャン が有効に働かない場合もある。 パッシブスキャンだとシステムに影響を及ぼす可能性が低い。
IoT ネットワーク	IoT 機器や IoT 機器を制御するコントローラが直接インターネットへ接続されている場合は対象外とする。 制御ネットワーク、フィールドネットワークにコントローラが接続されている場合、コントローラは対象とする。（コントローラ配下の IoT 機器は対象外）
オフライン	本ガイドラインの対象外（手段は台帳確認及び目視確認のみ）

表 10　収集方法について(1/2)

項番	手法	特徴	注意事項
①	制御システム資産台帳やベンダーからの納入仕様書	• 制御システムへの追加対応が不要である • 作成時点での OS 情報、設置場所、導入年月等詳細な情報が確認できる	• リアルタイム性がなく情報が古い可能性が高く、サイバー攻撃発生時において迅速な対応が取りづらい • ベンダー範囲外は制御システムオーナーが管理しないといけない • 増改造時は必ず更新をすること（ベンダーに依頼する）
②	目視確認（手作業）	• 資産の状況（オフライン等）に関わらず確認ができる • 設置場所が確実に把握できる	• 時間がかかる
③	監視画面（SCADA、HMI 等）	• リアルタイムでの稼働状況等がわかる	• 画面に表示されている情報以外は分からない • サイバー攻撃にて表示改ざんされた場合に気づけない
④	アクティブスキャン（認証型） ※1,2	• スイッチ設定の変更不要で実施可能である • エージェントと同様、取集可能な情報が多い	• 認証情報の管理が手間になる • 制御システムで実施する場合、制御システムに影響（システム停止、データ欠損など）が生じる可能性があるため、可用性に影響を及ぼさないよう留意が必要である

表 10 収集方法について(2/2)

項番	手法	特徴	注意事項
⑤	アクティブスキャン（非認証型）※2,3	• スイッチ設定の変更不要で実施可能である • 管理外の資産を発見できる • 空きポート、起動サービス等を発見できる	• PLC へ余計な通信が行かないよう調整が必要である • アクティブスキャン （認証型）、エージェントスキャンほど取得可能な情報が多くない • 制御システムで実施する場合、制御システムに影響（システム停止、データ欠損など）が生じる可能性があるため、可用性に影響を及ぼさないよう留意が必要である
⑥	パッシブスキャン	• 制御システムへの影響が少ない • 24 時間 365 日の監視が可能である	• 設置場所に通信が来ないと検知できない • 大量の通信の場合、パケットを拾えない場合がある • スキャン対象の制御システムにミラーポートがない場合、定期メンテ時に交換するなどが必要になる
⑦	エージェント	• 取得可能な情報が最も多い • 認証情報が不要である	• 端末にインストールする必要がある • コントローラにインストールできない（製品自体もない） • 稼働 OS が古い場合、早期のサポート期限切れリスクあり • 制御システムで実施する場合、制御システムに影響（システム停止、データ欠損など）が生じる可能性があるため、可用性に影響を及ぼさないよう留意が必要である

※1 RDP（Remote Desktop Protocol）を用いた確認方法などがある

※2 本ガイドラインにおいてアクティブスキャンは全て同一セグメントを対象にスキャンしていることを想定している

※3 SDN(Software Defined Networking)を利用すると、機器の物理的接続は変更せず、アクティブスキャンの到達範囲をコントロールでき、アクティブスキャンの自由度が増す。

■　収集方法毎の取得可能な情報一覧

表 11 では取得難易度、取得にかかる時間を考慮していないが、「資産台帳、納入資料書」「目視確認、手作業」は時間がかかるが多くの情報が取れる可能性が高い。それ以外の手法は収集できない情報も多いが素早く取得ができる。システム、ネットワークに応じて収集方法を組み合わせることで資産情報を効率よく収集することが可能である。

［凡例］

●：取得できる可能性が高い情報

▲：取得できる可能性が高いが、収集可能な資産種別が情報系資産に限定される場合がある

×：取得できない可能性が高い情報

―：項目ごとの注釈を参照

表 11　収集方法毎の取得可能な情報一覧

収集方法 / 資産情報項目	①資産台帳、納入仕様書	②目視確認、手作業	③監視画面	④アクティブスキャン（認証）	⑤アクティブスキャン（非認証）	⑥パッシブスキャン	⑦エージェント
資産名※1	●	●	●	▲	●	●	▲
資産種別	●	●	●	▲	×	●	▲
資産の持つ機能	●	●	×	▲	×	●	▲
回線種類	●	●	×	▲	×	×	▲
設置場所	●	●	×	×	×	×	×
接続先ネットワーク	●	●	●	▲	×	●	▲
管理ポートの接続先	●	●	×	▲	×	●	▲
操作 I/F の有無	●	●	●	▲	×	×	▲
USB ポート・通信 I/F 利用	●	●	×	▲	×	×	▲
媒体・機器接続の定常運用有無	●	●	×	×	×	×	×
無線機能の有無	●	●	×	▲	×	×	▲
定常稼働・非定常稼働	●	●	×	×	×	×	×
データの種類と経路	●	●	×	▲	×	●	▲
構築ベンダー、機器メーカー※2	●	●	×	▲	●	●	▲
OS の種類、バージョン	●	●	×	▲	●	●	▲
使用するプロトコル	●	●	×	▲	×	●	▲
セキュリティ対策※3	—	—	—	—	—	—	—
資産の重要度※4	—	—	—	—	—	—	—
資産の担当者※5	—	—	—	—	—	—	—
資産の責任者※5	—	—	—	—	—	—	—
IP アドレス	●	●	●	—※6	●	●	▲
MAC アドレス	●	●	×※7	—※6	●	●	▲

※1 IP アドレス、MAC アドレスといった端末が識別できる情報でも代替可能である
※2 MAC アドレスから機器ベンダーは取得可能である
※3 セキュリティ対策はセキュリティベンダー（制御システム導入ベンダーと同一の場合あり）等から提供された情報から確認する
※4 資産の重要度はリスクアセスメント時に決定するので、その際に台帳に追記する
※5 資産の担当者、責任者は資産導入時、組織再編成時に台帳に記入・更新をする
※6 既に取得済み（取得済みでないと認証型のアクティブスキャンができない）
※7 監視画面に MAC アドレスが表示されているケースは少ない

10 ツール紹介について

OS の標準コマンドやフリーツールだけでもある程度資産情報を収集できるため、参考情報としてツールの特徴、簡単な使い方について紹介する。なおアクティブスキャンとパッシブスキャンの注意点は 9 章を参照してほしい。

対応 OS については下記バージョンにて確認した。

Windows: Windows10 Pro バージョン 1909
Linux(Debian 系): Debian10.4
Linux(RedHat 系)：CentOS Linux release 8.1.1911 (Core)

【ネットワークスキャンツール】

表 12　ツール一覧(1/3)

項番	ツール名	対応 OS	コマンド／ソフトウェア	OS 標準／フリーツール	スキャン方法	取得可能な情報
1	Wireshark	Windows Linux	ソフトウェア	フリーツール	パッシブスキャン	キャプチャパケット内の MAC アドレス、IP アドレス、 ポート番号、プロトコル種別他
		パケットキャプチャソフト。キャプチャしたパケットの内容から MAC アドレス・IP アドレス・ポート番号表示および TCP/IP をはじめとした数多くのプロトコル解析機能がある。 ネットワークのトラフィック量が多い場面では Wireshark の動作が重くなり、キャプチャ漏れを起こしたり Wireshark がハングアップしたりする場合がある。この場合後述の tshark 等、より軽量なツールを使用する。 【インストール方法】 Windows 版: https://www.wireshark.org/download.html Linux 版（Debian 系）： sudo apt-get install wireshark Linux 版（RedHat 系）： sudo yum install wireshark インストール後、ユーザーを wireshark グループに追加する必要あり。 例）root 権限で gpasswd -a ユーザー名 wireshark				

表 12 ツール一覧(2/3)

<table>
<tr><th>項番</th><th>ツール名</th><th>対応 OS</th><th>コマンド／ソフトウェア</th><th>OS 標準／フリーツール</th><th>スキャン方法</th><th>取得可能な情報</th></tr>
<tr><td>2</td><td>arp-scan</td><td>Linux</td><td>コマンド</td><td>フリーツール</td><td>アクティブスキャン（非認証）</td><td>MAC アドレス、IP アドレス</td></tr>
<tr><td colspan="7">ホスト探索ツール。IP アドレス・MAC アドレス・MAC アドレスのベンダー名を一覧表示する。
nmap と比較してホストの発見に特化しており送出するパケットは arp request のみである。ネットワークへの負荷も比較的軽いと言えるが、アクティブスキャンに共通する特徴として、制御ネットワーク上で使用する際は注意が必要である。
例）arp-scan -I eth0 192.168.1.0/24（インターフェース eth0 を指定してスキャン）
【インストール方法】
Linux 版（Debian 系）：sudo apt-get install arp-scan
Linux 版（RedHat 系）：
①下記サイトから rpm ファイルをダウンロード
https://download-ib01.fedoraproject.org/pub/epel/7/x86_64/Packages/a/arp-scan-1.9.2-1.el7.x86_64.rpm
②perl と LWP がインストールされていない場合、下記インストールを実施
sudo yum install perl
sudo yum install perl-libwww-perl
③①でダウンロードした rpm ファイルのあるディレクトリで下記インストールコマンド実行
sudo rpm -ivh ./arp-scan-1.9.2-1.el7.x86_64.rpm</td></tr>
</table>

表 12 ツール一覧(3/3)

項番	ツール名	対応 OS	コマンド／ソフトウェア	OS 標準／フリーツール	スキャン方法	取得可能な情報
3	Nmap	Windows Linux	コマンド	フリーツール	アクティブスキャン（非認証）	MAC アドレス、 IP アドレス、 ポート番号、 OS・バージョン
		ポートスキャンツール。サービスアプリケーション検知機能や OS・バージョン検知機能等、多彩な機能を持つ。 arp-scan と比較して多機能である反面、arp,ping,DNS 参照等の多様なパケットを送出するため、制御ネットワーク上で使用する際は注意が必要である。 例）nmap 192.168.1.0/24（標準スキャン。arp,ping,DNS,TCP SYN ステルススキャンを実施する。） nmap -A 192.168.1.10（OS・バージョン検出を有効化する） 【インストール方法】 Windows 版：　https://nmap.org/download.html Linux 版（Debian 系）：　sudo apt-get install nmap Linux 版（RedHat 系）：　sudo yum install nmap				

【ネットワークスキャンを行う際に補助的に使用するツール】

表 13　補助ツール一覧（1/3）

項番	ツール名	対応 OS	コマンド／ソフトウェア	OS 標準／フリーツール	スキャン方法	取得可能な情報
1	ipconfig ifconfig ip	Windows Linux	コマンド	OS 標準	-	自ホストのネットワークインターフェース情報
		自ホストのネットワークインターフェース情報を確認するコマンド。ネットワークインターフェース名、IP アドレス等を確認できる。Linux(Debian)では ip。				
2	arp	Windows Linux	コマンド	OS 標準	-	自ホストの ARP テーブル情報
		自ホストの ARP テーブル情報を確認・追加・削除するコマンド。 例）arp -a（自ホストの ARP テーブル上の IP アドレス・MAC アドレスを一覧表示）				
3	netstat	Windows Linux	コマンド	OS 標準	-	自ホストと通信先の IP アドレス・ポート番号等、ネットワーク接続状態
		自ホストのネットワーク接続状態を確認するコマンド。mac では smbutil。				
4	ping	Windows Linux	コマンド	OS 標準	アクティブスキャン（非認証）	IP アドレス
		IP ネットワークにおいて相手先ホストへの到達可否を確認するコマンド。icmp echo request を送出する。アクティブスキャンに共通する特徴として、制御ネットワークで使用する際は注意が必要。				
5	tracert traceroute	Windows Linux	コマンド	OS 標準	アクティブスキャン（非認証）	IP アドレス、経路情報
		IP ネットワークにおいて相手先ホストまでの経路情報を取得するコマンド。Windows 版では icmp eho request、Linux 版では UDP パケットを送出する。アクティブスキャンに共通する特徴として、制御ネットワークで使用する際は注意が必要。				
6	nslookup	Windows Linux	コマンド	OS 標準	-	DNS 情報
		DNS サーバへドメイン名・IP アドレスの名前解決を要求するコマンド。				

表 13 補助ツール一覧（2/3）

項番	ツール名	対応 OS	コマンド／ソフトウェア	OS 標準／フリーツール	スキャン方法	取得可能な情報
7	dig	Linux	コマンド	OS 標準	-	DNS 情報
		DNS サーバへドメイン名・IP アドレスの名前解決を要求するコマンド。nslookup と比較して応答結果の加工がないため、より正確な情報を得られる。				
8	tcpdump windump	Linux Windows	コマンド	フリーツール	パッシブスキャン	キャプチャパケット内の MAC アドレス、IP アドレス、ポート番号、プロトコル種別他
		ネットワークパケットをキャプチャするコマンド。CentOS 等一部の Linux では OS に標準でバンドルされている。Windows 版は WinDump。 【インストール方法】 Windows 版： https://www.winpcap.org/windump/default.htm Linux 版（Debian 系）： sudo apt-get install tcpdump Linux 版（RedHat 系）： sudo yum install tcpdump				
9	tshark	Windows Linux	コマンド	フリーツール	パッシブスキャン	キャプチャパケット内の MAC アドレス、IP アドレス、ポート番号、プロトコル種別他
		Wireshark のコマンドライン版。 【インストール方法】 Linux 版（Debian 系）： sudo apt-get install tshark Linux 版（RedHat 系）： Wireshark と同時にインストールされる				

表 13 補助ツール一覧（3/3）

<table>
<tr><th>項番</th><th>ツール名</th><th>対応 OS</th><th>コマンド／ソフトウェア</th><th>OS 標準／フリーツール</th><th>スキャン方法</th><th>取得可能な情報</th></tr>
<tr><td rowspan="2">10</td><td rowspan="2">p0f</td><td>Linux</td><td>コマンド</td><td>フリーツール</td><td>パッシブスキャン</td><td>IP アドレス、ポート番号、
OS・バージョン</td></tr>
<tr><td colspan="5">パッシブ OS フィンガープリンティングツール。キャプチャしたパケットの内容から OS・バージョンを検知できる。
例）p0f -i eth0
【インストール方法】
Linux 版（Debian 系）：sudo apt-get install p0f
Linux 版（RedHat 系）：
①下記サイトから rpm ファイルをダウンロード
https://download-ib01.fedoraproject.org/pub/epel/7/x86_64/Packages/p/p0f-3.09b-1.el7.x86_64.rpm
②①でダウンロードした rpm ファイルのあるディレクトリで下記インストールコマンド実行。
sudo rpm -ivh ./p0f-3.09b-1.el7.x86_64.rpm</td></tr>
</table>

10.1　自動化ツールについて

資産情報の収集および資産台帳との突合を自動化する資産情報自動収集ツール（自動化ツール）を開発し、検証を行った。

10.1.1 自動化ツールの目的と位置付け

資産管理のやり方が分からない、手作業で管理している組織向けに以下の目的のもと開発した。

- 資産情報の収集と突合を自動化することでどれほど効果があるのか体験していただく
- 手軽に資産管理の自動化を検証することで自動化の理解度を深めていただく（商用製品導入検討時の参考にする）

商用製品との住み分けを表した図は以下の通りになる。

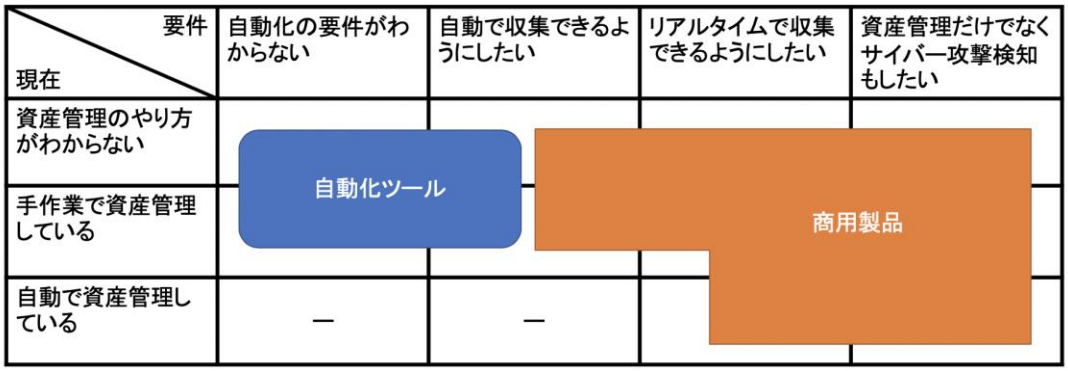

図 6　自動化ツールの位置付け

10.1.2 商用製品と比較した時の自動化ツールの特徴

以下のように手軽に検証することが可能

- アクティブスキャン、パッシブスキャンどちらも可
- 専用ハードウェア不要
- 日本語対応

10.1.3 自動化ツールの概要

ネットワーク経由で資産情報を収集し、台帳作成/更新および不正な端末、通信の検出が可能。

なおアクティブスキャンは制御システムの可用性に影響を及ぼす可能性があるため、使用開始時に警告表示される。

- 以下の OS にて動作する python 3.x 系プログラム（動作確認済み OS）
  ・macOS 10.14
  ・CentOS7
  ・raspbery pi Debian version 10.3
- アクティブスキャン （非認証型）、もしくはパッシブスキャンによって資産情報を収集できる
- スキャン実行時に台帳ファイル(CSV ファイル)を指定することで台帳ファイルとスキャン結果の比較が可能で、不正な IP アドレス、MAC アドレスなどを持つ端末を検出できる
- スキャン結果を CSV 形式で出力可能なため、台帳作成・更新が可能
- 取得および台帳作成/更新できるのは、前章で記載している「脅威を把握するために必要な資産情報」のうち、ネットワーク経由で取得可能な以下の資産情報項目とする

表 14　自動化ツールで取得可能な資産情報一覧

資産情報項目	簡易アクティブスキャン	詳細アクティブスキャン	パッシブスキャン※1
資産名(ホスト名)		●※2	●※2
IP アドレス	●	●	●
MAC アドレス	●	●	●
ベンダー情報	●	●	●
OS 種類、バージョン		●※3	●※3
通信先			●
通信プロトコル（ポート含む）			●
制御通信プロトコル固有詳細情報		●※4	

※1:スキャンするには通信が流れている必要がある。大量通信の場合、パケットを拾えない場合がある

※2:ホスト名はアクティブスキャンの場合は NetBIOS 名を取得しており、対象端末が未対応の場合は取得できない。パッシブスキャンの場合は DHCP、NBNS プロトコルから判定しているため通信が流れていない場合は判定できない。

※3:OS 種類、バージョンは TTL(Time To Live)から Windows 系、Linux or MAC 系、Unix or Network 機器系と簡単な判定のみ（判定できない場合は unknown）。

※4: BACnet のみ実装

自動化ツールの実行フローは以下の図のようになっている。

- 簡易アクティブスキャン では arp のみを実施している
- 詳細アクティブスキャン では arp に加えて、NetBIOS、PING を実施している
- 制御通信プロトコルスキャンでは正規の制御通信プロトコルを用いて情報収集を実施している（現時点では BACnet のみ）
- パッシブスキャンでは tshark を用いて pcap ファイルを作成後、それを読み取り解析を実施している
- PCAP スキャンは pcap ファルを読み込み、解析を実施している

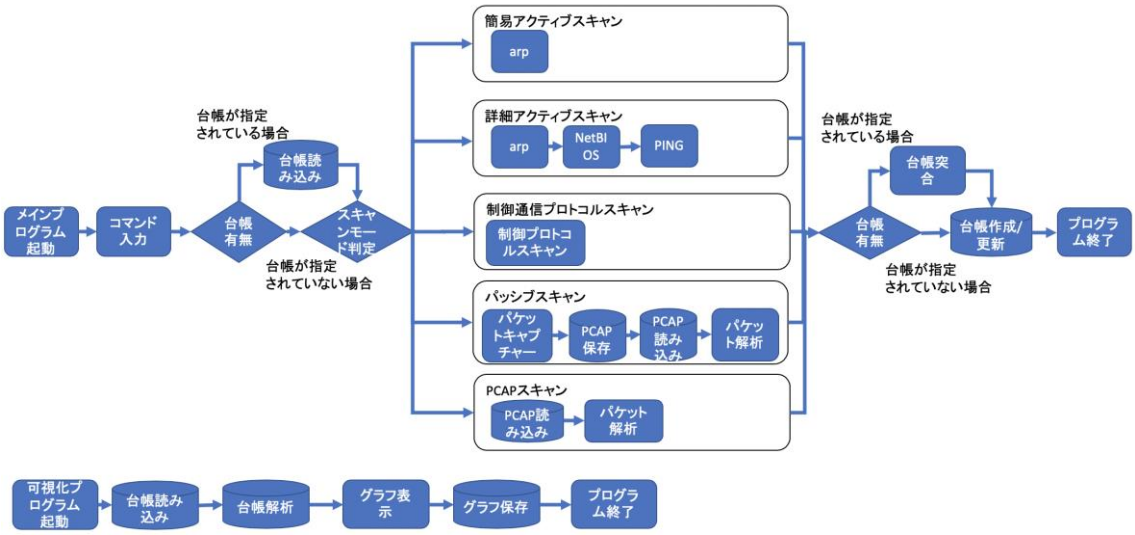

図 7　自動化ツールのフロー図

10.1.4 実行画面

メインファイルを python で実行後、コマンド入力して実行する（メインファイル起動時に引数入力で実行開始も可能）。例は簡易アクティブスキャン実行時とヘルプ実行時。

```
[redacted]$ python3 coe_assetmanagement_main.py
コマンドを入力してエンターを押してください
ass en0 192.168.0.0/24

###警告###

##アクティブスキャンは制御システムに影響を与える可能性がございます##
##利用者の自己責任のもと利用いただくことに同意いただける場合は実行ください##
##「yes」と入力後、Enterを押下すると##
##アクティブスキャンを実行します##
##同意いただけない場合はこのままEnterを押下してください##

yes
アクティブスキャン簡易モード（台帳なし）実行
[ArpAsset]
host= unknown :ip_src= 192.168.0.1 :mac= [redacted] :os= unknown :vendercode= [redacted] :mac_dst= unkno
wn :ip_dst= unknown :protcol= unknown :port_src= unknown :port_dst= unknown :communication= unknown :matchstatsu=
実行完了しました
```

図 8 実行画面（簡易アクティブスキャン ）

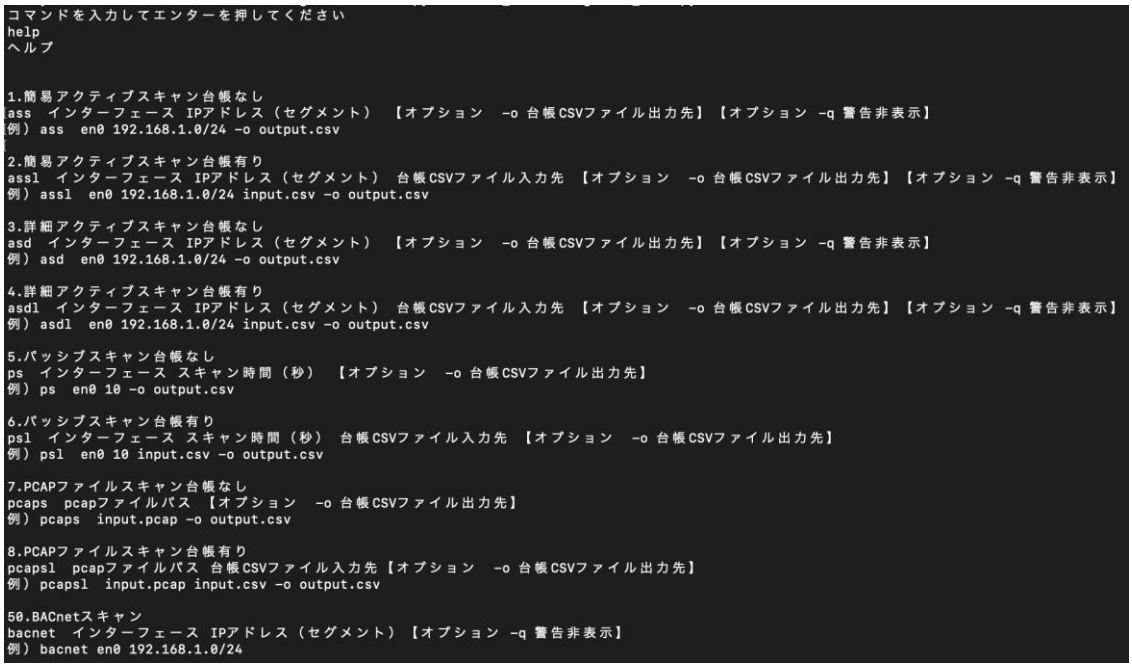

図 9 実行画面（ヘルプ）

10.1.5 実行結果

以下はパッシブスキャンを実施したときの出力結果※値はサンプル

hostname	ip_src	mac_src	vendercode	osname	ip_dst	protocol	port_src	port_dst	communication	status
hostA	192.168.1.10	aa:bb:cc:dd:ee:01	sampplevender	windows	192.168.1.25	UDP(4117),UDP(4114),BACnet-AF	411,447,808	4,117,411,447,808	192.168.1.10:4114-192.168.1.255:UDP(4117),	OK
hostB	192.168.1.11	aa:bb:cc:dd:ee:02	sampplevender	windows	255.255.255.	UDP(4117),UDP(4114)	4114	41,174,114	192.168.1.11:4114-255.255.255.255:UDP(411	OK
unknown	unknown	aa:bb:cc:dd:ee:03	sampplevender	unix or network	unknown	STP	unknown	unknown	unknown	OK
hostC	192.168.1.30	aa:bb:cc:dd:ee:04	sampplevender	windows	192.168.1.20	BACnet-APDU(47808),ARP	47808	47808	192.168.1.30:47808-192.168.1.209:BACnet-AF	OK
hostD	192.168.1.209	aa:bb:cc:dd:ee:05	sampplevender	windows	192.168.1.30	BACnet-APDU(47808),ARP	47808	47808	192.168.1.209:47808-192.168.1.30:BACnet-AF	OK
hostE	192.168.1.203	aa:bb:cc:dd:ee:06	sampplevender	windows	192.168.1.40	BACnet-APDU(47808),ARP,ICMP,I	478,081,750,054,129	47,808,175,001,900	192.168.1.203:47808-192.168.1.40:BACnet-AF	OK
hostF	192.168.1.40	aa:bb:cc:dd:ee:07	sampplevender	windows	192.168.1.20	ARP,BACnet-APDU(47808)	47808	47808	192.168.1.40:47808-192.168.1.203:BACnet-AF	OK
hostG	192.168.1.70	aa:bb:cc:dd:ee:08	sampplevender	windows	192.168.1.25	BACnet-APDU(47808)	47808	47808	192.168.1.70:47808-192.168.1.255:BACnet-AF	OK
hostF	192.168.1.12	aa:bb:cc:dd:ee:09	sampplevender	windows	192.168.1.25	BACnet-APDU(47808)	47808	47808	192.168.1.12:47808-192.168.1.255:BACnet-AF	OK
hostH	192.168.1.21	aa:bb:cc:dd:ee:10	sampplevender	windows	192.168.1.25	BACnet-APDU(47808)	47808	47808	192.168.1.21:47808-192.168.1.255:BACnet-AF	OK

図 10　スキャン機能の CSV 出力結果

またスキャン結果のネットワークトポロジー図を出力することが可能。過去の資産台帳と比較することで、図のように新規資産台帳にしかないデータは赤色、逆に古い資産台帳にしかないデータは緑色で表示することが可能で、目視でも変化に気づくことが容易。また MAC アドレスのみの表示、IP アドレスのみの表示も可能。

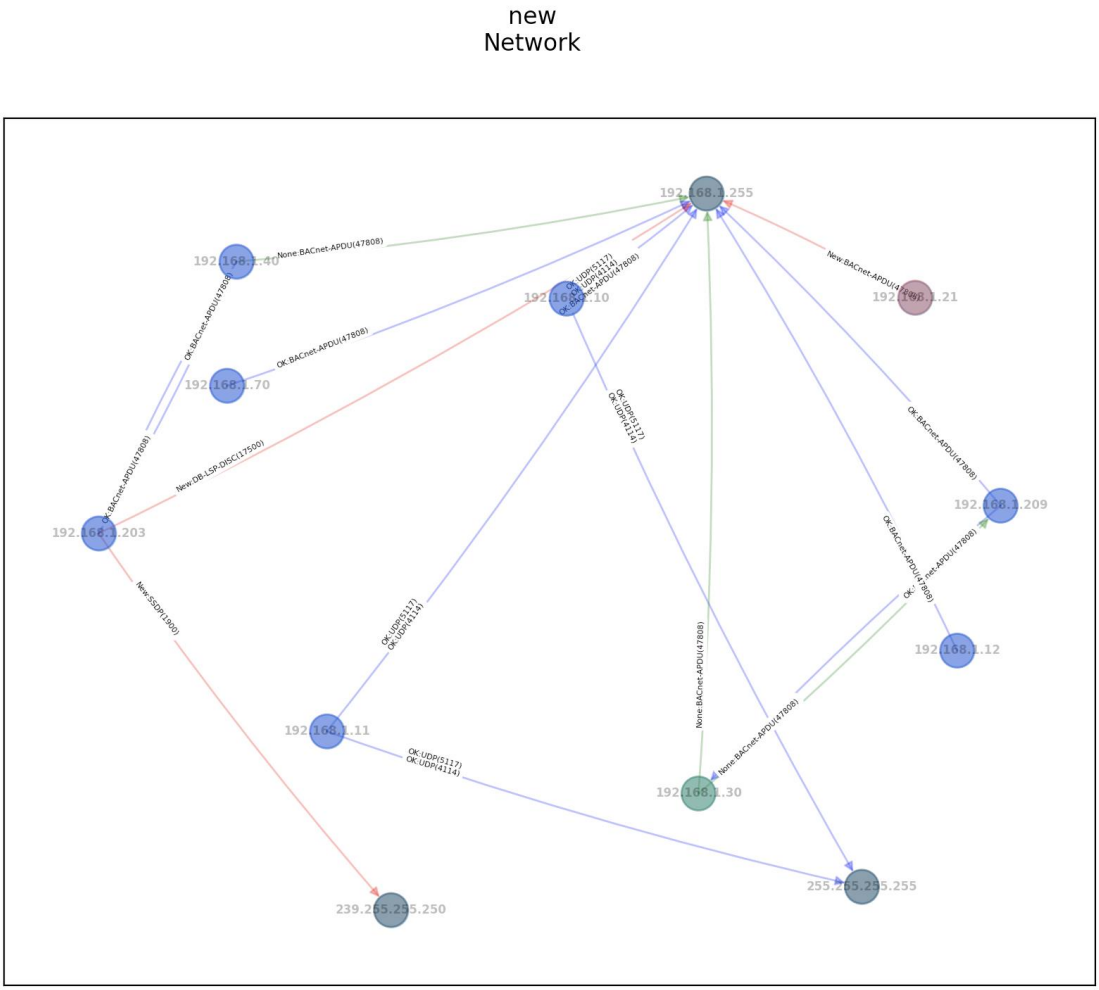

図 11　ネットワーク可視化機能の出力結果

さらに可視化機能は XML 出力ができ、外部ツール（例は Cytoscape を使用）を用いることでノードの移動、拡大・縮小やフィルタリング操作が可能のため可視性を上げることができる。例では新しい通信を赤く表示している。

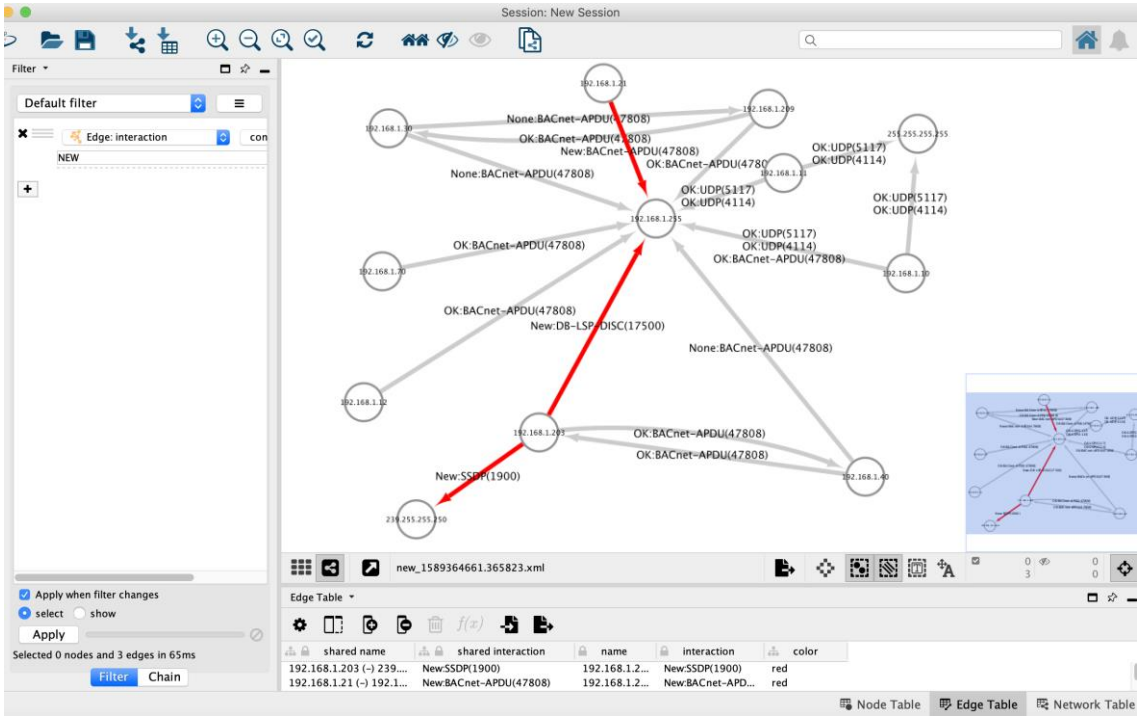

図 12 外部ツール（Cytoscape）での出力結果

10.1.6 検証内容

自動化ツールがある場合とない場合で、資産情報の取得時間および台帳作成/更新時間にどれだけ差が出るか比較を行う。検証項目は、自動化ツールで取得および台帳作成/更新可能な項目に絞る。

表 15　自動化ツール有無による比較項目

資産情報項目	比較項目	自動化ツール有り	自動化ツール無し
資産名（IP アドレス、MAC アドレスといった端末が識別できる情報で代替可）	●	ツールにてホスト名、IP アドレス、MAC アドレス確認。 ※ネットワーク資産は確認不可の場合あり	手作業
資産識別		手作業 ※通信経路のスイッチは個別確認が必要	手作業
資産の持つ機能		手作業	手作業
回線種類		手作業	手作業
設置場所		手作業	手作業
接続先ネットワーク	●	ツールにて確認可能	手作業
管理ポートの接続先		手作業	手作業
操作 I/F の有無		手作業	手作業
USB ポート・通信 I/F 利用		手作業	手作業
媒体・機器接続の定常運用有無		手作業	手作業
無線機能の有無		手作業	手作業
定常稼働・非定常稼働		手作業	手作業
データの種類と経路		手作業 ※ツールにて経路は確認可能（通信元：通信先：使用ポート、プロトコル）だがデータの詳細（プロセス値、制御コマンド等）は不明	手作業
構築ベンダー、機器メーカー	●	ツールにて機器メーカーは確認可能。構築ベンダーは手作業だが構築ベンダー情報は変わらないで更新確認は不要	手作業
OS の種類、バージョン	●	ツールにて確認可能	手作業
使用するプロトコル	●	ツールにて確認可能	手作業
セキュリティ対策		手作業	手作業

10.1.7 検証環境

- 制御ネットワーク（情報側）には、生産管理サーバ１台、OPC サーバ１台、オペレーターステーション１台がある
- 制御ネットワーク（制御側）には、OPC サーバ１台（情報側と同マシンで別 NIC）、オペレーターステーション１台（情報側と同マシンで別 NIC）、エンジニアリングステーション１台、PLC３台、HMI１台、アクチュエータ用コントローラ５台が接続されていおり、資産管理対象は合計１３台になる
- 両セグメント共にミラーポートが設置されている
- 本環境では１分で制御システムのプロセスが一巡する

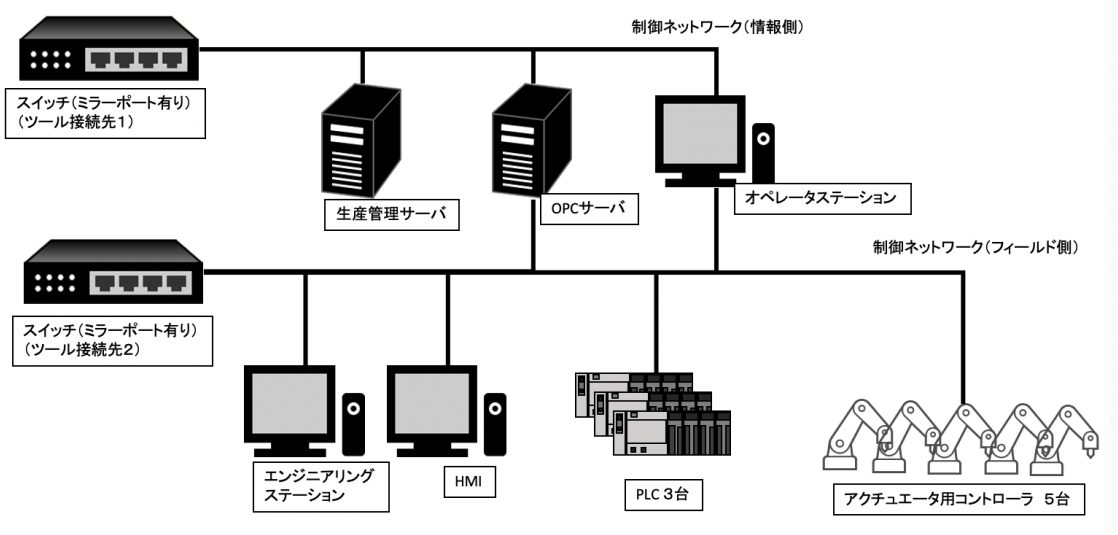

図 13　検証環境

10.1.8 検証結果

以下、自動化ツール実施有無による資産情報の収集および台帳作成/更新に要する時間を比較した結果になる。収集時間こそ差はあまりないが、台帳との突合が自動化することで圧倒的に早くなることがわかる。

表 16　検証結果

資産情報項目	比較項目	自動化ツール有り	自動化ツール無し
資産名(IP アドレス、MAC アドレスといった端末が識別できる情報で代替可)	●	アクティブスキャン 実施 2 分 4 秒（1 セグメント収集 1 分× 2 ＋台帳作成/更新 2 秒× 2）	arp-scan による確認 15 分（1 セグメント収集 1 分× 2 ＋台帳作成/更新 13 分）
接続先ネットワーク	●	パッシブスキャン実施 4 分 15 秒（2 セグメント分同時に収集 1 分＋解析 3 分 15 秒） ※1 分で約 53 万パケット 6 0 MB 収集	Wireshark による確認 26 分（パケット収集は上記「資産名」で合わせて実施）
構築ベンダー、機器メーカー	●	0 秒（上記、「接続先ネットワーク」取得時に併せて収集および台帳作成/更新確認）	Wireshark による確認 7 分（パケット収集は上記「資産名」で合わせて実施）
OS の種類、バージョン	●	0 秒（上記、「接続先ネットワーク」取得時に併せて収集および台帳作成/更新確認）	Wireshark による確認 7 分（パケット収集は上記「資産名」で合わせて実施）
使用するプロトコル	●	0 秒（上記、「接続先ネットワーク」取得時に併せて収集および台帳作成/更新確認）	Wireshark による確認 26 分（パケット収集は上記「資産名」で合わせて実施）
合計		6 分 19 秒	81 分

10.1.9 非対応機能

自動化ツールでは、以下に対応していない。

- MAC アドレスや IP アドレス、もしくは両方を詐称した機器（なりすまし攻撃）に気づけない
- オフライン端末（電源 OFF 等）は検知できない
- アクティブスキャンにおいては arp 機能に未対応（例：IPv6 機器、IP 未割り当て）の機器を検知できない
- パッシブスキャン、pcap ファイルのスキャンにおいて１パケット目のみ解析しない（実装に用いたライブラリ仕様）
- 常時監視をしていないため、スキャン時外の機器や通信を検知できない

10.1.10 総論

- 手作業でも Wireshark を使用すれば、資産情報の取得は可能。しかし目視による台帳との比較は非常に時間がかかる。目視の確認では抜け漏れのリスク、やり直しの可能性が常にあるので自動化可能なところは自動化が望ましい。
- 今回は１３台での検証だったが、台数が増えれば増えるほど収集に必要な時間差は広がる。検証者が Wireshark に慣れた者が実施したため、不慣れな場合や別の手段をとった場合、時間差はさらに広がると考えられる。
- 通信先やプロトコルを把握しておくことで許可リストの作成につなげることも可能。また新規の通信先やプロトコルを見つけた時に通信の流れを把握することが可能。
- 今回はミラーポートがある環境での検証だったが、実環境ではミラーポートが設置されていない環境もある。その場合、アクティブスキャンのみで一部資産情報だけでも自動収集するか、端末毎にツールを起動させて送受信パケットを取得する必要がある。またポートに空きがない場合も、その場合は LAN ケーブルを抜線して、インラインでパケットを収集するといった対応が必要になる。そのため制御システムを構築する際は資産情報が収集できるネットワーク構成を検討しておくことが望ましい。

11 製品検証について

本章では制御システムの資産情報を自動又は手作業で収集可能な商用のソフトウェア又はアプライアンス製品を稼働させて、検証をした結果を述べる。
※本章の製品とは資産情報を収集するソフトウェア又はアプライアンス製品とする。

11.1　目的

本プロジェクトおける製品検証の目的は次の 2 点である。

- 制御システムにおいて、製品毎に収集可能な資産情報を明確にする
- 検証を通して製品を導入する際に留意しなければいけないことを考える

11.2　検証対象

- パッシブスキャン製品
  制御システム向けの異常通信を検知する IDS(Intrusion Detection System)やネットワークトラフィックを分析することで情報を収集する DPI(Deep Packet Inspection)

- アクティブスキャン製品
  スキャン製品からパケットを送信して、受信した応答パケットから情報を収集する

本プロジェクトではパッシブスキャン製品とアクティブスキャン製品を混ぜた 5 製品と第 10 章の自動化ツールを対象として検証を実施した。

表 17　検証した製品のスキャン種別

製品	スキャン種別
A	パッシブスキャン
B	パッシブスキャン
C	パッシブスキャン
D	アクティブスキャン
E	パッシブスキャン＋アクティブスキャン
自動化ツール	パッシブスキャン＋アクティブスキャン

11.3　検証項目

検証項目は大きく 4 つの観点に着目して、合計 25 項目を設定した。

表 18　検証項目の分類

項番	分類	説明
1	情報取得	7 章にあるような収集すべき資産情報が取得できるか
2	検知能力	新規接続端末がいつ検知・把握できるか
3	構築・運用	構築や運用が現実的に可能であるか （例）レポートの出力可否、製品設定のバックアップ・リストア可否、操作性・見易さなど
4	その他	日本語対応・代理店の有無など

11.4　検証環境

検証環境は 10.1.7 の自動化ツールと同じ環境とした。（ツール接続先 1,2 に接続した）

11.5　検証手順

表 19　検証手順

項番	実施事項	目的
1	必要な環境を構築して製品を導入する	検証準備、構築に必要な条件・難易度を確認する
2	製品管理画面で初期状態を確認する	GUI・操作性を確認、取得可能情報の確認する
3	新規端末をネットワークに接続する	新規接続端末の検知を確認するための準備をする
4	製品管理画面で状態を確認する	新規接続端末の検知を確認する

11.6　検証結果

パッシブスキャン製品とアクティブスキャン製品で取得できる情報に差異があることが明確になった。

パッシブスキャン製品はネットワーク系の情報取得に強みがあり、アクティブスキャン製品は使用サービスの取得や導入容易性に強みがある。

また、同じパッシブスキャン製品でも情報の精度やユーザーインターフェースには差異がある。

表 20 検証結果(1/3)

項番	分類	検証項目	検証製品						評価基準
			A	B	C	D	E	自動化ツール	
1	情報取得	IP アドレス　取得有無	△	○	○	○	○	○	○：取得可能 △：条件付きで取得可能 ×：取得不可
2	情報取得	MAC アドレス　取得有無（IP を持つ機器）	○	○	○	○	○	○	○：取得可能 ×：取得不可
3	情報取得	MAC アドレス　取得有無（IP を持たない機器）	○	○	○	×	×	○	○：取得可能 ×：取得不可
4	情報取得	資産名　取得有無	○	○	○	△	○	○	○：取得可能 △：条件付きで取得可能 ×：取得不可
5	情報取得	資産の役割　取得有無	○	△	△	×	×	×	○：制御システム機器の役割(PLC,HMI など)を判別可能 △：制御システム機器の判別可能 ×：制御システム機器の判別不可
6	情報取得	接続先ネットワーク取得有無	○	○	○	×	×	○	○：取得可能 ×：取得不可
7	情報取得	データの種類と経路取得有無	○	○	○	×	×	○	○：取得可能 ×：取得不可
8	情報取得	使用するプロトコル取得有無	○	○	○	×	△	○	○：取得可能 △：条件付きで取得可能 ×：取得不可

表 20 検証結果(2/3)

項番	分類	検証項目	検証製品						評価基準
			A	B	C	D	E	自動化ツール	
9	情報取得	OS 種類、バージョン 取得有無	○	○	○	△	○	○	○：取得可能 △：条件付きで取得可能 ×：取得不可
10	情報取得	OS の修正パッチ適用状況　取得有無	×	×	×	×	×	×	○：取得可能 ×：取得不可
11	情報取得	使用サービス・アプリ 取得有無	×	×	△	△	△	×	○：取得可能 △：条件付きで取得可能 ×：取得不可
12	情報取得	初回検出日時　取得有無	○	○	○	×	○	×	○：取得可能 ×：取得不可
13	情報取得	最終検出日時　取得有無	○	○	○	×	○	×	○：取得可能 ×：取得不可
14	検知能力	新規端末設置の検出 検知までの時間	○	○	○	×	○	△	○：リアルタイム検知可能 △：スキャン時に自動検知可能 ×：手作業で既存台帳と比較が必要
15	構築	設置方法（導入容易性）	△	△	△	○	○	○	○：ネットワーク構成が変更不要 △：ミラーポートが必要 ×：ネットワークが構成変更必要
16	構築・運用	制御プロトコルとの混在（アクティブスキャン時の弊害）	-	-	-	○	○	○	○：弊害は確認できなかった ×：弊害あり

表 20 検証結果(3/3)

項番	分類	検証項目	検証製品						評価基準
			A	B	C	D	E	自動化ツール	
17	運用	ユーザインターフェース	○	△	○	○	○	×	○:資産情報を 1 画面で一覧表示可能 △:資産情報を一覧表示可能だが、表示に難あり ×:資産情報を一覧表示できない
18	運用	ネットワーク構成の表示・出力	○	○	○	×	×	○	○：表示可能 ×：表示不可
19	運用	アセット一覧のデータ出力	○	○	○	○	○	○	○：出力可能 ×：出力不可
20	運用	レポートの出力	○	○	○	×	×	×	○：機能あり ×：機能なし
21	運用	ツール更新、バージョンアップの可否	○	○	○	○	○	×	○：機能あり ×：機能なし
22	運用	製品設定のインポート・エクスポート可否（設定のバックアップ・復旧が容易か）	○	○	○	×	○	×	○：機能あり ×：機能なし
23	運用	イベントログ保有量、保有期間	不明	不明	不明	-	○	×	○：1 ヶ月以上保存可能 ×：1 ヶ月未満
24	その他	日本語対応	×	×	×	○	○	○	○：対応している ×：対応していない
25	その他	日本語代理店	○	○	○	○	○	×	○：あり ×：なし

11.7　総論

- ほとんどの製品で主だった情報の取得が可能であったが、一部の製品では資産と認識できるのはプライベート IP アドレス(192.168.xxx.xxx など)のみで、その他の IP アドレスは機器一覧に表示されないことがあった。
  そのため、プライベート IP アドレス以外の IP アドレスを利用している環境では期待する動作が得られない。製品導入の際に、導入環境での事前検証が重要であることを改めて確認できた。
- アラート・レポートの形式や内容は製品によって大きく違いが見られたため、望むアラートやレポートが得られるかどうかは導入を検討する際の考慮ポイントになる。例えば、得られた情報を元にリスクアセスメントを実施する際には、資産情報を CSV などの加工できる形で正確に出力できることが望ましい。
- パッシブスキャン製品は資産の役割を自動判定するが、情報が不正確か大雑把な役割表示（Computer や OT Device など）であった。また、製品独自の判別がされているため、学習に必要な期間や精度にはバラつきがあった。
  ただし、制御システム導入時の台帳や納入仕様書で補完できるので、製品での取得優先度は低い。
- パッシブスキャン製品はミラーポートの事前構築が前提のため、実環境での検証が難しい場合もある。また、全ての制御システムを監視するためには、その分のミラーポート構築が必要になる。不審な挙動を検知・アラートすることもパッシブスキャン製品の大きな役割なので、重要度の高い制御システムから導入していくことが望ましい。
  ミラーポートが既にある場合や構築が容易な環境である場合は、資産特定のために一時的に製品を使用することも可能である。
- アクティブスキャン製品は、制御システムへの可用性影響を確認する必要があるが、ミラーポート構築が不要で環境構築・運用が容易であるので、資産管理の自動化第一歩として機器の IP アドレス、MAC アドレスの管理から始める場合に推奨できる。

12 資産管理の成熟度モデルについて

制御システムの資産管理における成熟度モデルの評価は、組織がサイバーセキュリティリスクをどのように捉えているか、また、そうしたリスクを管理するためにどのようなプロセスが存在しているかを示す一助となる。

なお、制御システムにおける資産管理の成熟度モデルは下記のガイドラインや資料を参考に作成している。

- 重要インフラ分野向けのサイバーセキュリティフレームワークである『NIST Cyber Security Framework v1.1』を基にこの成熟度モデルは作成されている
- 『NIST CSF』では様々なプロセスの中でサイバーセキュリティリスクマネジメントの段階を『ティア』で定義しており、『ティア』の判断には既存の成熟度モデルを活用するように記載されている
- 成熟度モデルの作成においてはこの『ティア』をベースに『NIST CSF』の参照文献でもある『COBIT』の成熟度内容も参考に、本ガイドラインで定義した資産管理の取り組みを基に作成した
- サイバーセキュリティリスクをどのように管理するか、資産管理の側面で自組織の取り組みを支援するものである

【使用方法】

基本的な使用方法としては、自組織の資産管理の成熟度レベルの現状状況を評価し、想定するあるべき状況とのギャップ分析に活用することで、自組織の資産管理の取り組みを支援するものである。より高位のレベルに進むことが推奨されるのは、費用対効果分析の結果、サイバーセキュリティリスクの低減が実現可能で、費用効率も高くなることが示された場合である。

成熟度レベルの評価については、次章で説明する[チェックリスト]を活用してほしい。尚、［チェックリスト］の[評価]欄の L1～L4 の選択肢の考え方については、本成熟度モデルの成熟度レベルと整合しており、資産管理内容を満足できる場合はそのレベルに達していると評価できる。

資産管理内容を満足するためには手段の項目を参照し、得られる効果と課題から自組織の資産管理の側面での取り組みを向上させ、サイバーセキュリティリスク管理の一助としてもらいたい。

表 21　成熟度モデル

チェックリストレベル	成熟度レベル	内容 資産管理内容	手段 情報取得方法	効果	課題
essential	L1：レベル 1 資産情報を部分的に管理している	資産の一覧が作成できている。セキュリティを意識した資産情報が不足している。	システム構成図、メーカー納入仕様書を用いて資産の情報を手作業で収集している。	資産の有無を確認できる資産リスト作成が可能となる。	リスクアセスメントを実施するための資産情報が不足している。
	L2：レベル 2 必要な資産情報を管理している	本ガイドラインに定義した収集すべき資産情報を管理している。	レベル 1 同様	IPA 分析ガイド範囲のリスクアセスメントをするための管理が可能となる。	手作業が多く、資産情報を管理する工数がかかる。
middle	L3：レベル 3 資産情報の自動収集による管理	本ガイドラインに定義した収集すべき資産情報を一部もしくはすべてを自動で収集している。	レベル 2 に加えて、資産情報を収集できるツールを用いている。	許可していない資産の自動検知ができる様になる。 資産情報の重複がなくなる。	資産情報の管理が属人的で非効率なため、資産台帳の更新が自動化できていない。
high	L4：レベル 4 資産管理の最適化	本ガイドラインに定義した収集すべき資産情報を自動化で管理している。	レベル 3 に加えて、資産台帳を自動更新できるツールを用いている。また資産台帳を一つのシステムで統合管理している。	資産台帳が最適化管理され、最新の組織の状況を適用できリスクマネジメントの質の向上が可能となる。	この状況を維持・改善していくこと

13 チェックリストについて

本ガイドの内容を組織内で実践するにあたり、制御システムの資産管理をセキュリティの観点で行う上でのチェックリストを作成した（別紙）。12 章の成熟度モデルと合わせて、自組織での資産管理において充足している項目を洗い出し、何を充実させるべきかを明らかにする一助として欲しい。

なお、本ガイドのチェックリストは下記のガイドや資料を参考に作成している。

- 重要インフラ分野向けのサイバーセキュリティフレームワークである『NIST Cyber Security Framework v1.1』を基にこのチェックリスト は作成されている
- 小項目の作成にあたっては『NIST CSF』では ISO-27000 や CIS CSC 等の様々な参照文献があるが、主に情報システムの内容であることを鑑み、その中でも最も親和性の高い『NIST SP800-53 rev4』を参考に作成した

【使用方法】

基本的な使用方法としては、各小項目に対し自組織の資産管理状況がその項目を満たしているのかを[チェックリスト]シートの[評価]欄に記載していき、すべての評価が完了した後、[評価シート]で組織内の充足度を確認するというものである。

ただし、チェックリスト活用にあたっては以下の点に注意して欲しい。

- [小項目]内にさらに a、b、c・・・等の項目がある場合はすべて満たした場合に、その項目にチェックがつくことになる
- チェックリストを活用するにあたり[小項目]内に、**［指定：組織が定めた、制御システム資産の効果的な説明責任を果たすのに必要と考えられる情報］**等の記載がある場合がある。その場合は、チェックを行う前に事前にその内容を組織内で決定しておく必要がある

  [評価]欄の L1～L4 の選択肢の考え方については、**「12 資産管理の成熟度モデルについて」**の章を参照して欲しい

14 資産管理体制と資産管理の流れについて

本章では資産管理を実施するにあたって、組織として留意する点、また実際に資産台帳を更新する流れについて記載する。

14.1 資産管理体制について

組織として資産管理を実施するにあたってまず留意すべき点は以下の通りになる。

- 資産管理における管理対象範囲、管理項目を定義する
- 上記定義を定期的もしくは重大な事象発生（自組織に関連するサイバーセキュリティ事件の発生等）時に見直す
- 資産管理を実施する体制（実担当者、責任者。以降「管理体制」）を明確化する
- 管理体制は定期的もしくは重大な事象発生時に見直す
- 管理体制は必要に応じて社外関係者も含めて明確化（文書化、契約締結含む）させる
- 管理体制の社内外含めた関係者への周知
- 管理対象範囲においてハードウェア、ソフトウェアの追加、削除、変更について資産台帳へ反映する仕組みの構築と運用遵守
- 定期的にチェックリストを用いて自社の資産管理の実施状況を確認し、管理体制を改善していく

14.2　資産管理台帳作成･更新の流れについて

実際に資産台帳を作成・更新する場合の主な流れは以下の通りになる。

表 22　資産台帳作成・更新の流れについて

項番	項目	内容
1	資産台帳入手	前回作成した資産台帳を入手する。ない場合はベンダーから納入仕様書等、資産情報を入手する。 そのため日頃から台帳の保存場所の把握、ベンダー(もしくは保守業者)から情報入手するための窓口を把握しておく必要がある。
2 -a	制御ネットワーク（情報側）に繋がった機器の資産情報入手	(2-b とは平行で実施) 使用できるツール、製品の選択肢が多く、制約も緩い。組織のセキュリティポリシーに応じて自動収集を行い、不足分は目視確認（手作業）を行う。アクティブスキャン、エージェントは制御システムに影響（システム停止、データ欠損など）が生じる可能性はゼロではないため留意が必要。
2 -b	制御ネットワーク（フィールド側）とフィールドネットワークに繋がった機器の資産情報収集	(2-a とは平行で実施) 推奨する収集手段として監視画面、パッシブスキャンがある。なおパッシブスキャンをするためには事前に必要なパケットが収集できるようにミラーポートが設置されている必要がある。アクティブスキャン、エージェントは制御システムに影響（システム停止、データ欠損など）が生じる可能性があるため、可用性に影響を及ぼさないよう留意が必要。自動収集できない項目については目視確認（手作業）を行う。
3	収集した資産情報を資産台帳と突合する	自動化しておくことで人的ミスの排除、業務効率化が実現できる。
4	資産台帳との差分の調査・対応	資産台帳と差分が生じた場合、必要に応じて以下のような対応が必要となる。 ・オペレーションミス等による台帳更新のミスの場合：台帳を更新し、再発防止を行う ・許可されていない端末を検知した場合：端末を制御ネットワークから隔離を行う。 ・許可されていない通信（プログラム）を検知した場合：プログラムの停止を行う。
5	資産台帳の更新および関係者周知	資産台帳を更新し、更新結果について関係者へ周知を行う。

15 留意・検討すべき事項について

以下のような項目についても検討が必要と思われる。

- インストールされていない（実行形式）のアプリ管理（実行した瞬間であれば既存の資産管理ソフトで検知可能）
- サプライチェーンの部品、ソフトウェアの管理
- 資産管理の効率化を実施した場合の、後工程（リスクアセスメント、リスクマネジメント）への影響検証

16 総括

本ガイドラインは、制御システムにおいて資産管理の必要性を認識いただくだけでなく、何を収集すべきか、収集した情報が何に使用されるのか、どのような収集手段があるのか等、理解を深めていただける内容となっている。

また自動化ツールや製品検証結果を通して、自動化の有効性や製品導入時の仕様検討に役立てていただける内容となっている。

収集すべき情報が多いように感じるが、いずれもサイバーセキュリティ対策をする上で必要不可欠と考えられる情報のため、自動化可能な情報は自動化を実施して効率良い資産管理を目指していただきたい。

本ガイドラインが、資産管理の実施を促進し、より良いリスクアセスメント、リスクマネジメントにつながり、皆様のセキュリティ対策が向上されることを期待する。

17 参考文献

制御システムのセキュリティリスク分析ガイド　第２版
https://www.ipa.go.jp/files/000080712.pdf

Cyber Security Framework version1.1
https://www.ipa.go.jp/files/000071204.pdf

NIST Special Publication 800-53 Rev4
https://www.ipa.go.jp/files/000056415.pdf

経営者のための情報セキュリティ対策-ISO31000 から組織状況の確定の事例-
https://www.jnsa.org/result/2018/west_tebiki/data/section01.pdf

スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス
https://www.ipa.go.jp/files/000073490.pdf

Cytoscape

https://cytoscape.org/

【免責事項】

下記【著作権】欄に記載の各著作権等保有者（以下、「各権利者」）は、本ガイドラインおよびチェックリスト（以下、両者を「本作品」と総称）の利用に起因または関連して利用者に生じたトラブルや損失、損害等に対して、一切の責任を負いません。

【注意事項】

本記載内容は各権利者のうち専ら下記【著作権】欄に記載の本プロジェクトの見解に基づいております。如何なる意味においても独立行政法人情報処理推進機構産業サイバーセキュリティセンターの見解を反映するものではありません。

【著作権】

本作品に関する著作権その他すべての知的所有／財産権は、「独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 3 期生 資産管理プロジェクト（以下、「本プロジェクト」）」及び本作品中に利用した下記各イラスト制作者等に帰属します。

- CMAN(https://sozai.cman.jp/info/)
- ICOOON MONO(https://icooon-mono.com/license/)

利用者は、上記【免責事項】、【注意事項】のすべての内容に同意する場合に限り、本作品を、自己利用または、自身の所属組織での内部利用のため必要な範囲で複製し、或いはそのサーバー上に搭載して閲覧等に供することができます。これらの範囲を超える利用は、各権利者の明示の同意がない限り、禁止されています。

【作成者】

独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム 3 期生　資産管理プロジェクトメンバー
古城　巧太　　（東ソー株式会社）
平　芳久　　（株式会社 PFU）
大原　健太郎　（横河電機株式会社）
小河原　聡　　（通研電気工業株式会社）
佐藤　佑　　（北陸電力株式会社）
柴崎　健　　（日本原子力防護システム株式会社）
杉本　芳剛　　（パナソニック株式会社）
高野　悟　　（東京ガス株式会社）
棚橋　宣康　　（中部電力株式会社）
長浜　佑介　　（日本電気株式会社）
矢口　貴史　　（株式会社 SUBARU）
湯浅　琢麻　　（株式会社豊田自動織機）

【監修】

独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム　講師
満永　拓邦
目黒　有輝
藤本　万里子
松田　亘

【版管理】

2020 年 6 月 29 日	初版


Industrial Cyber Security Center of Excellence
ICSCoE