制御システムにおける資産管理ガイドライン【活用の手引き】

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

本資料の内容は下記の通りである

1. 本ガイドラインの背景・目的

本ガイドラインの背景・目的

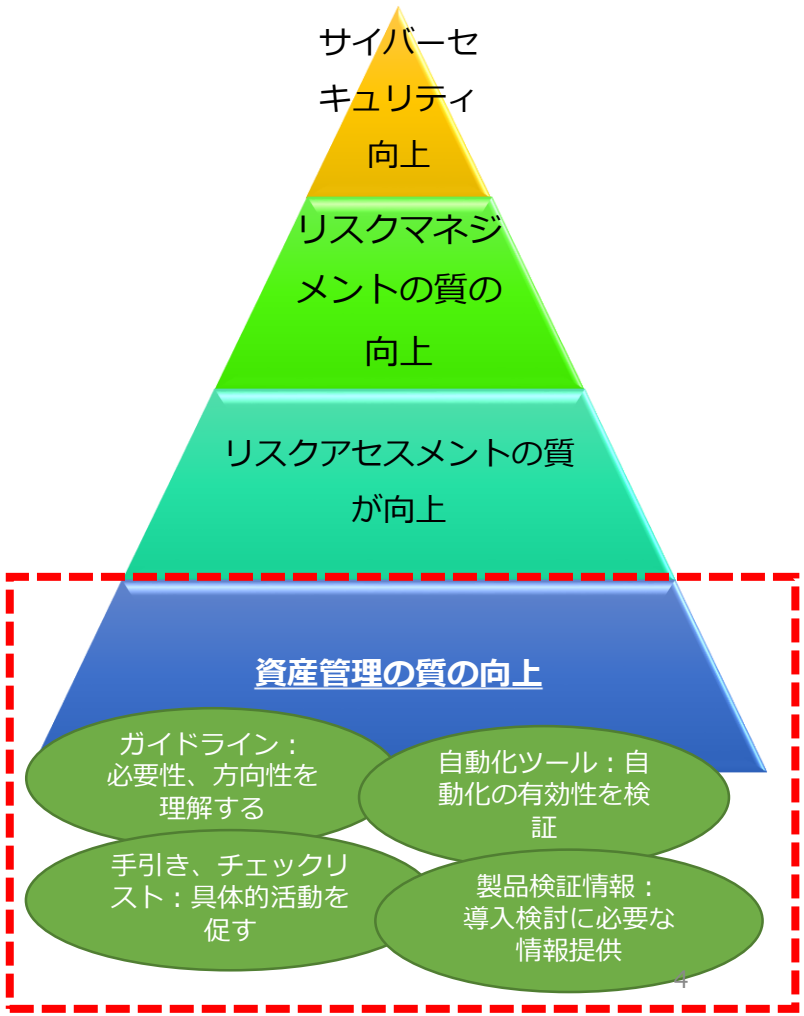
増大する制御システムのサイバーセキュリティリスクを資産管理の効率化によって低減させることを目的としたガイドライン及び資産管理自動化ツール、製品検証情報である

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、サイバーセキュリティリスクの増加につながっている。増大するサイバーセキュリティリスク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り、リスクマネジメントを実施するにはISO3100で定義されている「組織の状況を確定」する必要があり、そのためには資産管理が必要である。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の必要（保護資産の明確化）とあるが、制御システムの資産管理方法について具体的な方法と課題について触れているガイドラインは見受けられない。

目的

制御システムに適した資産管理に関するガイドライン、手引きやチェックリスト、自動化の有効性検証、商用製品における資産管理機能の検証結果をまとめ、企業のサイバーセキュリティ向上を目指す。



2.『制御システムにおける資産管理ガイドライン』の活用の手引き

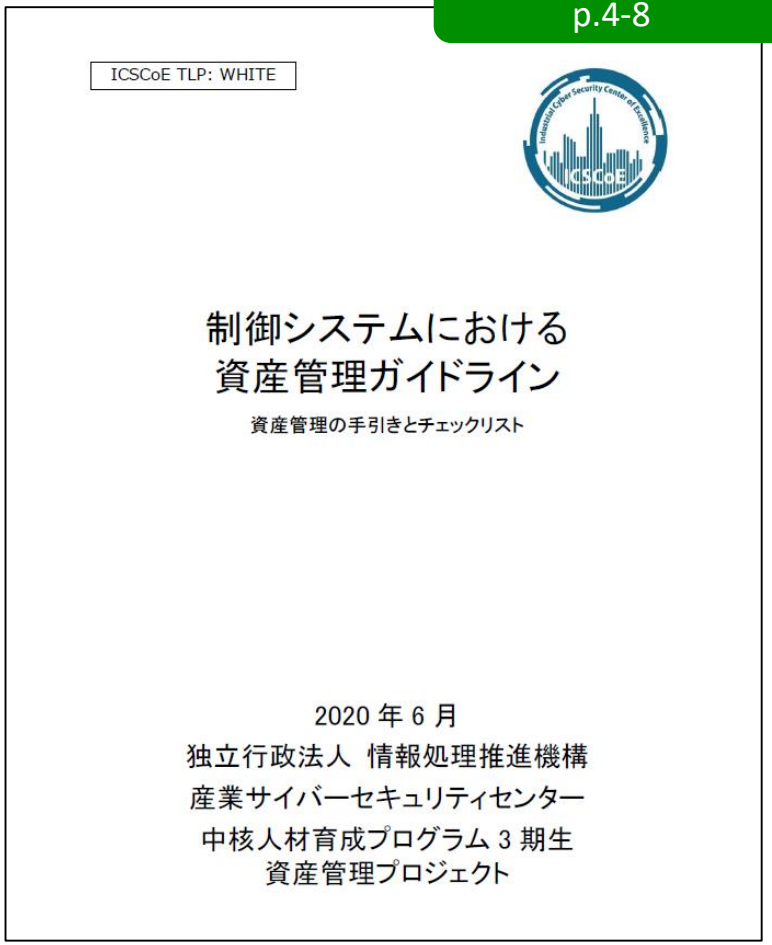
ガイドラインの概説(1章～3章)

1章～3章については、本ガイドラインに関する目的と活用方法を提示し、本ガイドラインの利用を促している

ガイドライン本編
p.4-8

1章　概要
2章　本ガイドラインの目的
3章　本ガイドラインの活用方法

- 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）
  - 脅威情報と資産情報（5章、6章、7章、8章）
  - 資産情報の収集方法（9章、10章、11章）
  - 資産管理の成熟度と評価（12章、13章）
  - 資産管理の手引き（14章）


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

資産管理の位置付け(4章)

本章では、セキュリティ対策における資産管理の位置づけを確認し、資産管理の必要性を示している

４章　資産管理の位置付け

- ISO31000*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、この整理が素早く、適切にすることが、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。
- 資産管理は、この整理を素早く、適切に意思決定するためのセキュリティ対策の土台である。

*ISO31000　リスクマネジメント規格

ガイドライン本編
p.9-10

4　セキュリティ対策における資産管理

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。

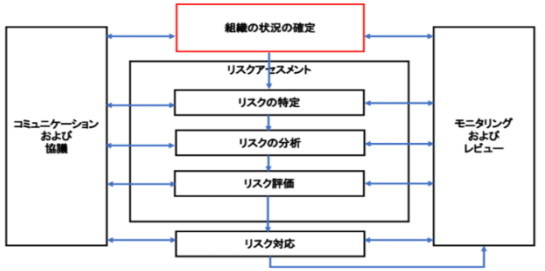


図 3　ISO31000 リスクマネジメントプロセス

他にも IEC62443 や NIST、NISC 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。

資産情報と脅威情報（5章～8章）

制御システムに対する脅威情報を具体的にし、本ガイドラインで推奨する収集すべき資産情報との関連づけにより、セキュリティ対策に繋がる資産管理を理解する

ガイドライン本編
p.11-24

5章　資産管理対象の範囲

- 資産管理対象とする制御システムの範囲を紹介している。

6章　制御システムにおける脅威とは

- セキュリティ対策につながる資産管理を実現するために制御システムに対する脅威を紹介している。

7章　収集すべき資産情報について

- 本ガイドラインで推奨する、収集すべき資産情報を紹介している。

8章　資産情報と脅威の関係性

- 資産情報と制御システムに対する脅威の関係性を紹介している。脅威に応じた資産情報を管理することにより、潜在的な脅威・顕在化した脅威を迅速に検知する。

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－接続
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	●					●	
無線妨害	●				●（※2）	●	
盗聴	●					●	

制御システムにおける脅威と資産情報の関係性を表にまとめた

資産情報の収集方法(9章～11章)

資産情報の収集方法や収集方法毎に取得可能な情報を説明し具体的な手引きも内容に盛り込んでいる

ガイドライン本編
p.25-54

9章　資産情報の収集方法について

- 資産情報の収集方法について、制御システムやNW種別に応じた収集方法を紹介している（右図）

10章　ツール紹介について

- 資産情報収集に利用できるOS標準コマンドやフリーツールの使用方法と特徴について、およびサブプロジェクトで開発した資産情報収集の自動化ツールについて紹介している

11章　製品検証について

- 資産情報を収集可能な商用製品について、収集可能な情報と、導入の際の留意事項について検証した結果を紹介している

表 11　収集方法毎の取得可能な情報

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	—	—	—	—	—	—	—

資産情報の収集方法とそれ毎に取得可能な情報を検証し、表にまとめた

成熟度モデル(12章)

成熟度モデルは、チェックリストと合わせてギャップ分析に活用でき、自組織の資産管理レベルを客観的に評価できる

ガイドライン本編
p.55-56

12章　資産管理の成熟度モデルについて

- 後述のチェックリストと合わせて、自組織がどの程度成熟しているかを客観的に評価できる
- 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

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

チェックリスト(13章)　1/2

チェックリストは、制御システムの資産管理を具体的にどの程度実施できているかを評価し、現状と目標のギャップ分析に活用できる

ガイドライン本編
p.57　及び別紙

制御システムセキュリティ観点からの資産管理チェックリスト

項番	大項目	項番	小項目	参照元 (SP800-53)	チェックリストレベル	評価
1	自組織内の物理デバイスとシステムが、カタログ作成されている	1-1　制御システム資産の一覧	下記の通り制御システム資産の一覧を作成し文書化している a 現行の制御システムを正確に反映している b その制御システムネットワーク内に正式に登録されている範囲に含まれる、すべての資産（フィールド機器は対象外）を対象としている ※収集すべき資産情報についてはガイドラインを参照のこと c リスクアセスメントやインシデント対応等ための調査や報告に必要と考えられる程度に詳細レベルになっている d ［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］を含んでいる	CM-8	essential	L2
		1-2　一覧のレビュー・更新	制御システム資産一覧を［指定：組織が定めた頻度で］レビューし、更新している。	PM-5	essential	L2
		1-3　責任に関する情報	制御システム資産一覧の情報に、資産の管理に責任のある個人（責任者及び担当者）を［選択（１つ以上）：氏名・地位・役職］によって特定できる手段を含める。	CM-8(4)	essential	L2
		1-4　資産変更に伴う更新	資産のインストールや削除の際に、また、制御システムのアップデートの際に、その一環として制御システム資産一覧を更新している。	CM-8(1)	middle	L3
		1-5　許可されていない資産の自動検知	下記の通り許可されていない資産を自動で検知し、対応を行っている a 制御システム内に許可されてない資産（ハードウェア）が存在する場合に検知できる、自動化されたメカニズムを［指 b 許可されてない資産が検知された場 ［選択（１つ以上）： ・そうした資産によるネットワーク ・それらの資産を切り離す ・［指定：組織が定めた職員または役			

『NIST CyberSecurity Framework』と『NIST SP800-53 rev4』を参考に項目を作成した

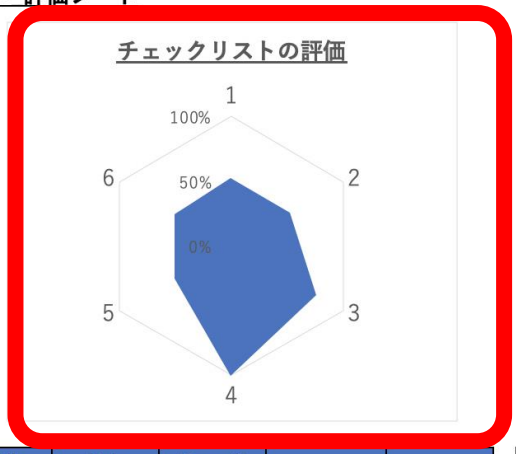
チェックリスト(13章)　2/2

チェックリストは、制御システムの資産管理を具体的にどの程度実施できているかを評価し、現状と目標のギャップ分析に活用できる

制御システムセキュリティ観点からの資産管理チェックリスト　評価シート

【レベルの凡例とポイント】

レベル	内容	評価	ポイント
essential	資産情報を部分的に管理している	L1	1
	必要な資産情報を管理している	L2	2
middle	資産情報の自動収集による管理	L3	3
high	資産管理の最適化	L4	4



【チェックされた項目数とポイント合計】

大項目	内容	essential		middle	high	チェック項目数計	ポイント合計	比率	(参考)満点
		L1	L2	L3	L4				
1	自組織内の物理デバイスとシステムが、カタログ作成されている	0	3	2	0	5	12	52%	23
2	自組織内のソフトウエアとアプリケーションが、カタログ作成されている	0	3	2	0	5	12	52%	23
3	組織内の通信とデータフロー図が、作成されている	1	1			2	3	75%	4
4	外部情報システムが、カタログ作成されている			1		1	3	100%	3
5	資産がそれらの分類、重要度、ビジネス上の価値に基づいて優先順位が付けられている								
6	従業員全体のサードパーティの利害関係者に対するサイバーセキュリティの役割と責任が確立されている								

レーダチャートで自組織にどの項目の取り組みができており、できていないかを「視覚的」に評価できるようにした

資産管理の手引き(14章)

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

ガイドライン本編
p.58-60

14章　資産管理体制と資産管理の流れ

- 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

表 22　資産台帳作成・更新の流れに

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。