『制御システムのセキュリティリスク分析ガイド』と国際規格との比較

説明資料

令和 6 年 12 月

独立行政法人情報処理推進機構

更新履歴

2024 年 12 月 10 日	初版

目次

1. 本調査の概要 5

2. 背景と目的 5

3. 対象読者 5

4. 内容 5

① リスク分析に関連する主な標準やガイドラインについて 5

② 制御システムのセキュリティリスク分析ガイドのスコープ 7

③ リスクアセスメントの必要性 9

④ 制御システムのセキュリティリスク分析ガイドのプロセス 9

⑤ 制御システムのセキュリティリスク分析ガイドで採用している解析手法と ISO/IEC 31010 での分類 13

⑥ NIST SP 800-37 と制御システムのセキュリティリスク分析ガイドのフレームワークの比較 15

⑦ IEC 62443-3-2 と制御システムのセキュリティリスク分析ガイドの手順の比較 16

⑧ NIST SP 800-30(Rev.1) と制御システムのセキュリティリスク分析ガイドの分析プロセスの比較 17

⑨ ETSI TS 102 165-1 V.5.2.5 (2020-01)と制御システムのセキュリティリスク分析ガイドの分析ステップの比較 18

5. まとめ 19

6. 参考資料 21

図目次

図 1 制御システムのセキュリティリスク分析ガイドのスコープ（点線）..... 7
図 2 評価指標とリスク値の算定方法 10
図 3 制御システムのセキュリティリスク分析ガイドの分析プロセス詳細.....11
図 4 制御システムのセキュリティリスク分析ガイドの分析プロセス概要.....12
図 5 ISO/IEC 31010 の分類とリスク分析ガイドの分析手法.....13
図 6 SP 800-37 リスクマネジメントフレームワークとの比較 15
図 7 IEC/PAS 62443-3 のリスクの考え方 16
図 8 IEC 62443-3-2:2020 のリスクアセスメントのワークフロー 16
図 9 SP800-30 リスクアセスメントプロセスとの比較 17
図 10 ETSI TS102-165-1 のプロセスとの比較 18
図 11 リスク分析を視点とした国際規格とリスク分析ガイドのスコープ概念図.....20

表目次

表 1 制御システムのセキュリティリスク分析ガイドの分析手法と評価指標の関係....10

1. 本調査の概要

IPA が発行する『制御システムのセキュリティリスク分析ガイド』の分析手法と国際的な規格やガイドラインに記載されるリスクアセスメント手法との比較について解説する。本資料では、脚注は上付き番号（例 [1]）、巻末の参考資料は[ ]付き番号（例 [1]）で表している。

2. 背景と目的

IPA では、制御システムのセキュリティリスク分析ガイドの分析手法に関して、この分析手法が国際的な規格やガイドラインに対しどのような位置付けになるかの質問を受ける事がある。そこで、本文書では、制御システムのセキュリティリスク分析ガイドに記載される詳細リスク分析手法と、リスクアセスメントに言及する国際規格 ISO/IEC 27000 シリーズ、IEC 62443 シリーズや NIST[1] SP 800-30 等との比較を実施し、評価項目の類似性や違いについて明確にする。

3. 対象読者

グローバルな観点からのリスク分析を必要とする分析者。

4. 内容

以下に IPA の制御システムのセキュリティリスク分析ガイドの考え方(フレームワーク)、解析手法と解析手順を各種の国際的な基準やガイドライン、フレームワークと照らし合わせて説明を行う。

① リスク分析に関連する主な標準やガイドラインについて

国際的に参照されている標準やガイドラインで IPA の制御システムのセキュリティリスク分析ガイドと関連のある主な資料とその大まかな位置付けを以下に説明する。

i. IEC 31010:2019 Risk management - Risk assessment techniques [1]
（英和対訳版では、「リスクマネジメント-リスクアセスメント技法」）
リスクマネジメントで利用されるリスクアセスメントの手法について種類と適性が記載されている。
IEC 31000 シリーズは事業に関する広範囲のリスク全般を扱っている標準となる。

ii. ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy

[1] NIST: National Institute of Standards and Technology（米国立標準技術研究所）

Protection - Guidance on managing information security risks [2]
情報システムのセキュリティマネジメンプロセスについて記載されている。

iii. IEC 62443-2-1:2024 Edition 2.0 Security for industrial automation and control systems -Part 2-1:Security program requirements for IACS asset owners [3]
産業用オートメーション及び制御システムのセキュリティを保つためのアセットオーナー向けの要求事項について記載されている。

iv. IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design(英和対訳版では「産業用オートメンション及び制御システムのセキュリティ-第 3-2 部:システム設計のセキュリティリスクアセスメント」) [4]
産業用オートメーション及び制御システムのセキュリティのリスクアセスメントの手順について記載されている。

v. NIST SP 800-30 Rev.1 Guide for Conducting Risk Assessments [5] (IPA の対訳版では、「情報セキュリティリスクアセスメント実施の手引き」 [6])
米国連邦政府の情報システムのリスクアセスメント実施方法について記載されている。

vi. NIST SP 800-37 Rev.2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [7] (IPA の英和対訳版[6]では、「情報システム及び組織のためのリスクマネジメントフレームワーク セキュリティ及びプライバシーのためのシステムライフサイクルアプローチ」)
米連邦政府機関向けに規定された、組織と情報システムのためのリスクマネジメントフレームワーク。

vii. ETSI[2] TS102 165-1 V5.2.5 (2022-01) CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) [8]
ETSI が定める詳細リスク評価アプローチ方法。

以降の説明では、読者の可読性を高くするため、タイトルに和訳がある場合和訳を

[2] European Telecommunications Standards Institute

記して説明を行う 。

② **制御システムのセキュリティリスク分析ガイドのスコープ**

以降の説明の前提として、制御システムのセキュリティリスク分析ガイドのスコープを明確にしておく。ISO/IEC 27005:2022 では、ISO Guide73[3]を参照し、リスクマネジメントはリスクアセスメントとリスク対応(Risk Treatment)があり、リスクアセスメントにはリスク特定、リスク分析、リスク評価があると説明されている。

一方、IPA の「制御システムのセキュリティリスク分析ガイド」では、主にリスク分析の手順についての説明がされているが、7章ではリスクの評価について説明し、3～4章ではリスクの特定について触れている。このスコープを図にすると以下の様になる。

(また、IEC 27005:2022 のリスクマネジメントプロセスには、コミュニケーション、協議などの広範囲なプロセスも含まれているが、リスク分析ガイドではそれらには触れていない)

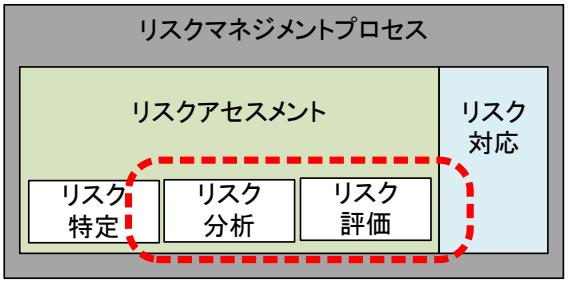

図 1 制御システムのセキュリティリスク分析ガイドのスコープ(点線)

[3] ISO Guide 73 は現在では Withdrawn となっている

【コラム】 ガイドブックとガイドライン

IPA の制御システムのセキュリティリスク分析ガイドの紹介をしていると、しばしば、またガイドラインが追加されたのかとの質問を受ける事がある。サイバーセキュリティに関するガイドラインは ISO,IEC の国際規格や NIST CSF(Cybersecurity Framework)、CPSF(経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク)、業界毎のガイドラインなど多数存在する。こういった多数のガイドラインが存在する状況に困惑している担当者も少なからずいると思われる。しかしながら、制御システムのセキュリティリスク分析ガイドは、「ガイドライン」ではなく「ガイドブック(手引き書)」である。既存の規格やガイドラインで要求されているリスク分析の手順について解説しているガイドブックという位置付けにある。
セキュリティに関しての詳細リスク分析を行う具体的な手順の参考書として利用していただきたい。

③ リスクアセスメントの必要性

IEC 62443-2-1:2024 Edition 2.0 Security for industrial automation and control systems -Part 2-1: Security program requirements for IACS asset owners

では、制御システムのアセットオーナーのためのセキュリティプログラムの要求事項を定義している。この中で、要求事項に対するリスクの評価に関する項があり、サイバーセキュリティリスクの決定は通常 IEC 62443-3-2 に沿って進めるとされている。

④ 制御システムのセキュリティリスク分析ガイドのプロセス

IPA が発行する制御システムのセキュリティリスク分析ガイドで採用している 2 つの詳細リスク分析手法においてリスク値の算出に用いる評価指標は制御システムのセキュリティリスク分析ガイド p.29 の表 2-2(本文表 1)に記すものであり、これらの指標をマトリクスに適用してリスク値を算定すると説明している。

表 1 制御システムのセキュリティリスク分析ガイドの分析手法と評価指標の関係

リスク分析手法	評価指標			
	資産の重要度	事業被害	脅威	脆弱性
資産ベースのリスク分析	○	―	○	○
事業被害ベースのリスク分析	―	○	○	○

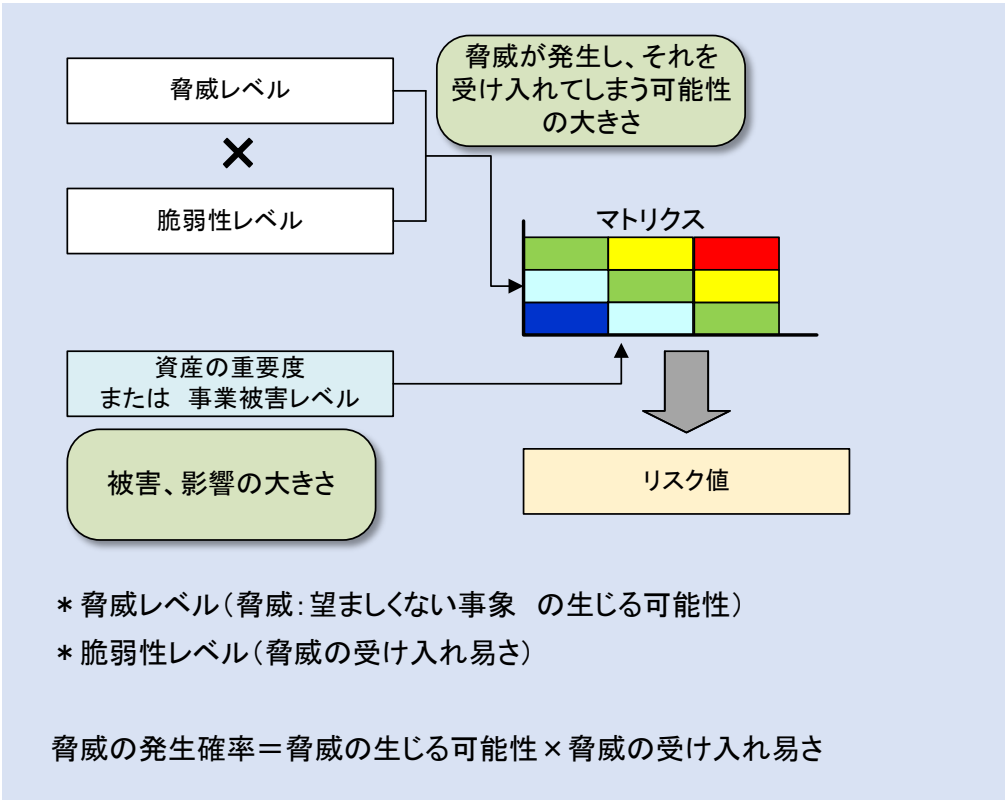

図 2 評価指標とリスク値の算定方法

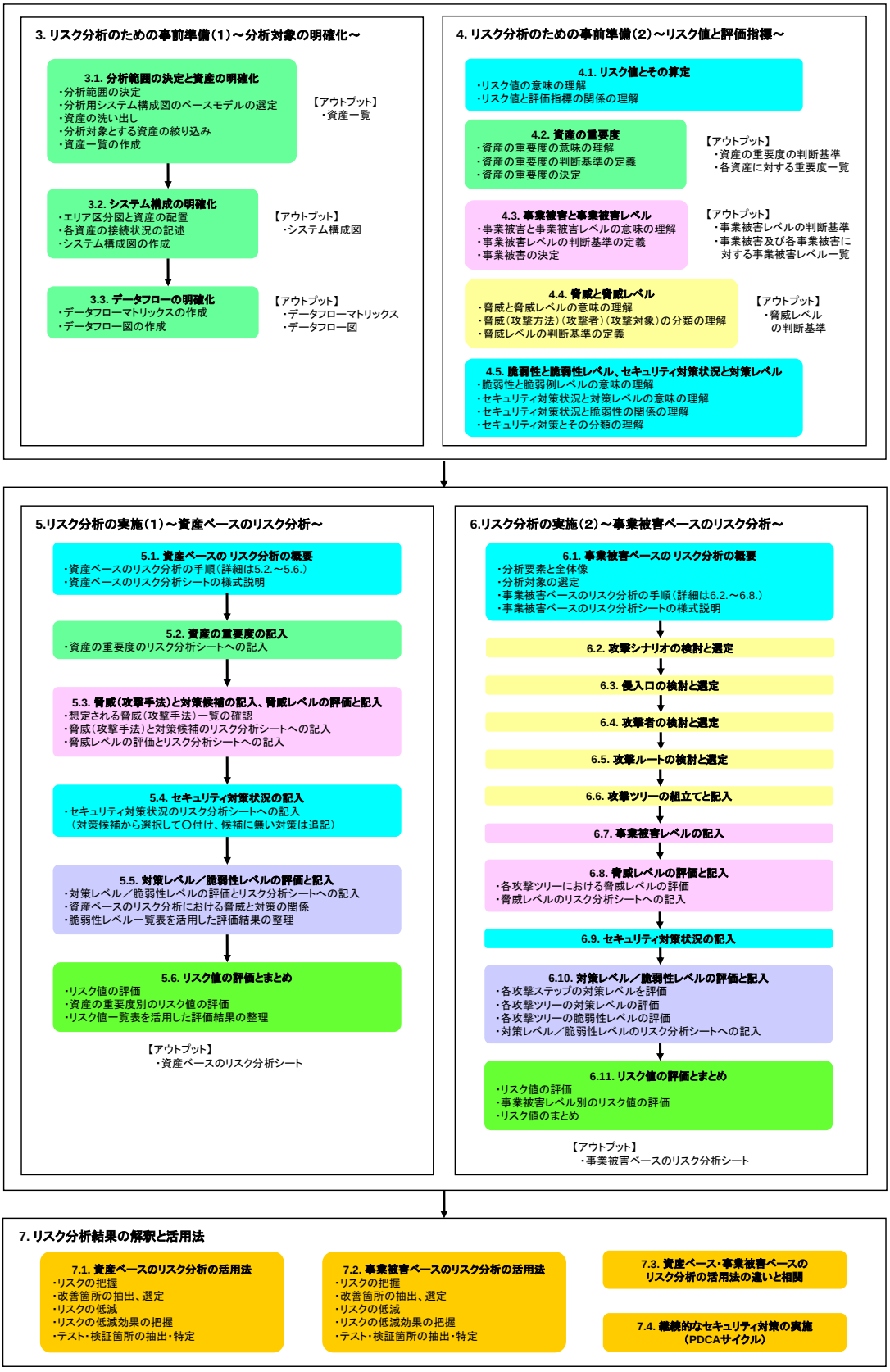

図 3 制御システムのセキュリティリスク分析ガイドの分析プロセス詳細

図 3 のプロセスを整理し、評価指標のフローを付け加え図 4 として記す。(赤点線は評価指標のフロー)

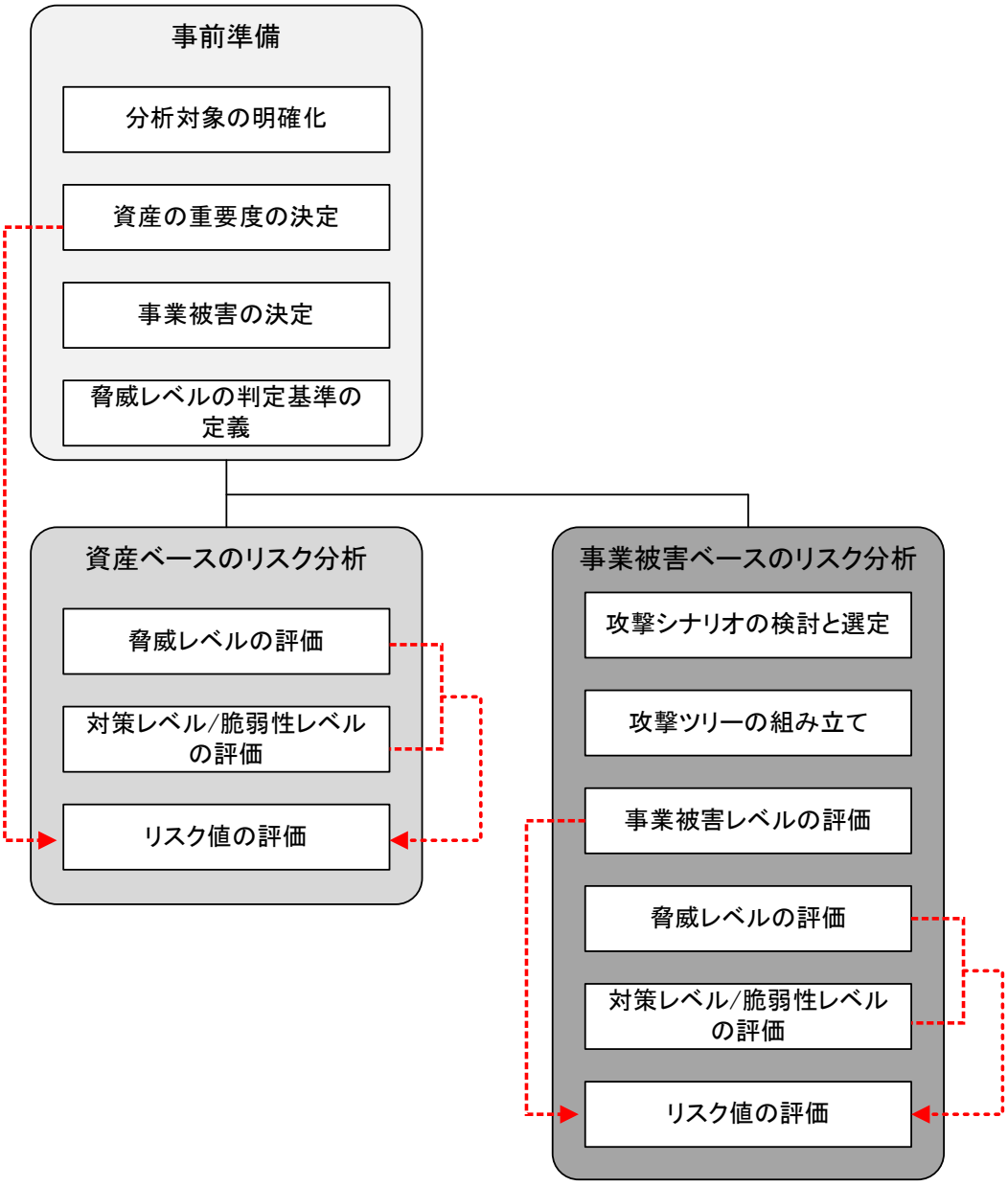

図 4 制御システムのセキュリティリスク分析ガイドの分析プロセス概要

⑤ 制御システムのセキュリティリスク分析ガイドで採用している解析手法と ISO/IEC 31010 での分類

事業被害ベースのリスク分析に関して、制御システムのセキュリティリスク分析ガイド p27 に、シナリオベースの分析であり、その解析手法は

・攻撃ツリー解析（ATA:Attack Tree Analysis）

*ATA は主に安全等に関する解析手法 FTA(Fault Tree Analysis)と類似の構造を持った情報セキュリティに関して用いられる解析手法

・イベントツリー解析(ETA：Event Tree Analysis)

の両方を採用している。

これらの解析手法は、ISO/IEC 31010 の附属書 A 技法の分類の項の、表 A.3 ISO 31000 プロセスへの技法の適用性 の中に、

・シナリオ分析

・事象の木解析（ETA）

・故障の木解析(FTA：Fault Tree Analysis)

等が挙げられており、これらに相当する。

また、資産ベースのリスク分析は、リスクの大きさに影響する指標として、資産の重要度を決定し、リスクの生じやすさを脅威レベルと脆弱性レベルという指標の組み合わせを用いている、この類似の解析手法は、同じく表 A.3 に記載されている Risk indices(リスク指標)が挙げられる。

ISO/IEC 31010	リスクアセスメントプロセス				
	リスク特定	リスク分析			リスク評価
		結果	発生確率	リスクレベル	
FTA	A	NA	SA	A	A
ETA	A	SA	A	A	NA
シナリオ分析	SA	SA	A	A	A

リスク分析ガイド（点線）

A:applicable; SA: strongly applicable; NA: not applicable

図 5 ISO/IEC 31010 の分類とリスク分析ガイドの分析手法

【コラム】CSF2.0 におけるリスクアセスメントの記載

NIST が発行している CSF(Cybersecurity Framework) 2.0 [9]では、リスクアセスメントは CSF のコアにあるカテゴリーの一つ(ID,RA)であり、「サイバーセキュリティリスクを把握するために、脅威、脆弱性、可能性、影響を用いて固有のリスクを理解し、リスク対応の優先順位付けを行う。」と記載されている。制御システムのセキュリティリスク分析ガイドでは、脅威と脆弱性から可能性を見積もり、事態の重要度/影響度からリスク値を算定する。制御システムのセキュリティリスク分析ガイドのリスク値の算定と同様の指標を用いていると解釈できる。

⑥ NIST SP 800-37 と制御システムのセキュリティリスク分析ガイドのフレームワークの比較

NIST SP 800-37 組織と情報システム(プロセス制御システムも含む)のためのリスクマネジメントフレームワーク(以下 RMF と略す) では、組織と情報システムに適用するために策定されている。RMF では、リスク分析を含むリスクマネジメント全体をカバーするものであり、一方の制御システムのセキュリティリスク分析ガイドは、図 1 に記した通りリスク分析だけでなく広くリスクマネジメント(リスク特定/リスク評価/リスク対応)も含んでいる半面、組織やプライバシーリスクに関してはは言及してはいない。このように一部のスコープは異なるが、NIST SP 800-37 の 1.PREPARE に記載される内容を比較すると図 5 のように対応している。

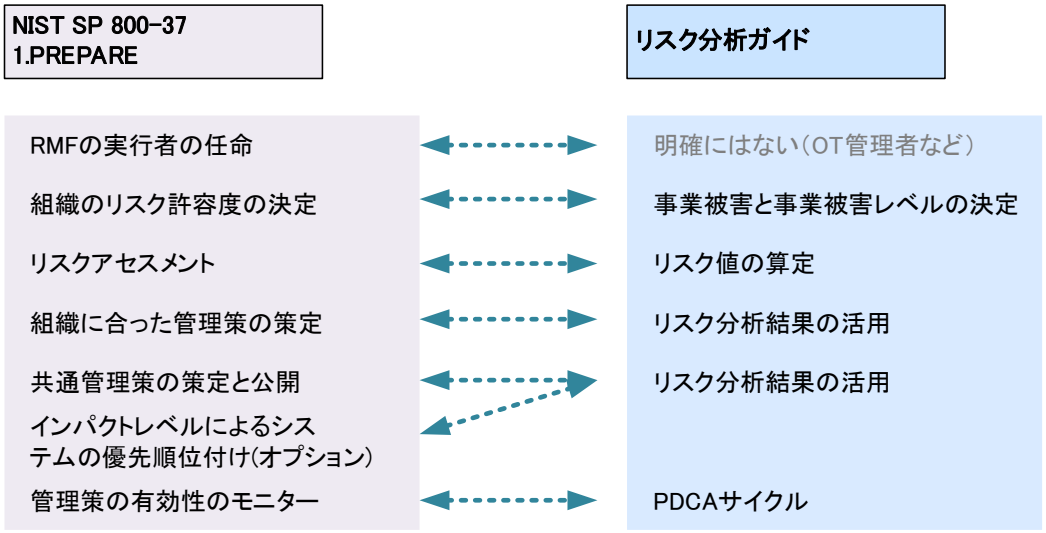

図 6 SP 800-37 リスクマネジメントフレームワークとの比較

⑦ IEC 62443-3-2[4] と制御システムのセキュリティリスク分析ガイドの手順の比較

2008 年に、IEC/PAS 62443-3 (PAS: PUBLICLY AVEILABLE SPECIFICATION PRE-STANDARD)が発行され、その中で、リスクは ISO Guide73 で「事象の発生確率とその結果の組み合わせ」で定義されていると記載されている[8]。

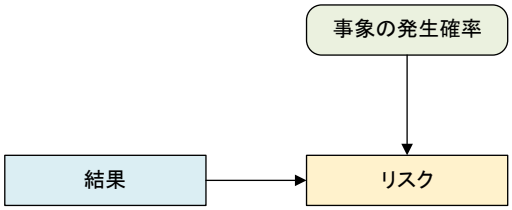

図 7 IEC/PAS 62443-3 のリスクの考え方

2017 年に初版が発行された IPA の制御システムのセキュリティリスク分析ガイドでは図 2 に示したように、脅威レベルと脆弱性レベル、つまり、脅威(望ましくない事象)の発生確率＝脅威の生じる可能性×脅威の受け入れ易さとして計算し、事業被害(または重要度)との組み合わせでリスク値を算定している。

2020 年に発行された IEC 62443-3-2:2020 では IEC/PAS 62443-3 の考えを受け継ぎ、制御システムのゾーン又はコンジットごとの詳細なサイバーセキュリティリスクアセスメントのワークフローとして、脅威を識別し、脆弱性を識別し、その結果から未軽減の起こりやすさを決定する、さらに脅威が実現した場合の結果および影響を決定してその組み合わせでサイバーセキュリティリスクを決定すると記載されている。

更に、リスクランクを確立するためのツールとして1つの軸に起こりやすさ、2 つ目の軸に重大度を示すリスクマトリクスを紹介している。

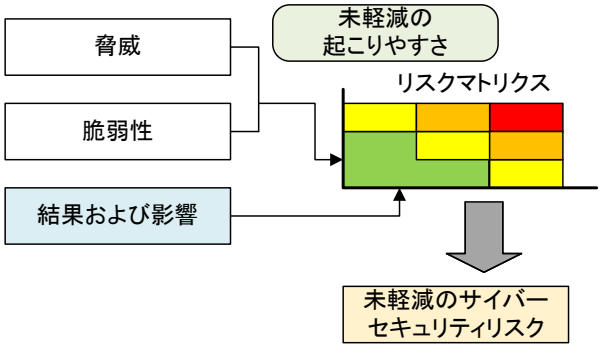

図 8 IEC 62443-3-2:2020 のリスクアセスメントのワークフロー

[4] IEC 62443-3-2 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design

[5] IEC PAS 62443-3 は ISO Guide73 ともに既に Withdrawn(廃止)となっている

⑧ NIST SP 800-30(Rev.1) と制御システムのセキュリティリスク分析ガイドの分析プロセスの比較

NIST SP 800-30 Guide for Conducting Risk Assessments（リスクアセスメントの実施の手引き） では、リスクアセスメントのプロセスに関して説明がされている。このプロセスを制御システムのセキュリティリスク分析ガイドのプロセスと比較したのが図 8 になる。

この図の、SP 800-30 における発生の可能性とは、リスク分析ガイドの脅威レベル（脅威が発生する度合い）×脆弱性レベル（その脅威を受け入れてしまう度合い）の考え方は同じである。

また、分析アプローチとして、Impact-oriented と Threat-oriented があると言及されており、これはリスク分析ガイドの ATA/ETA と類似したアプローチである。

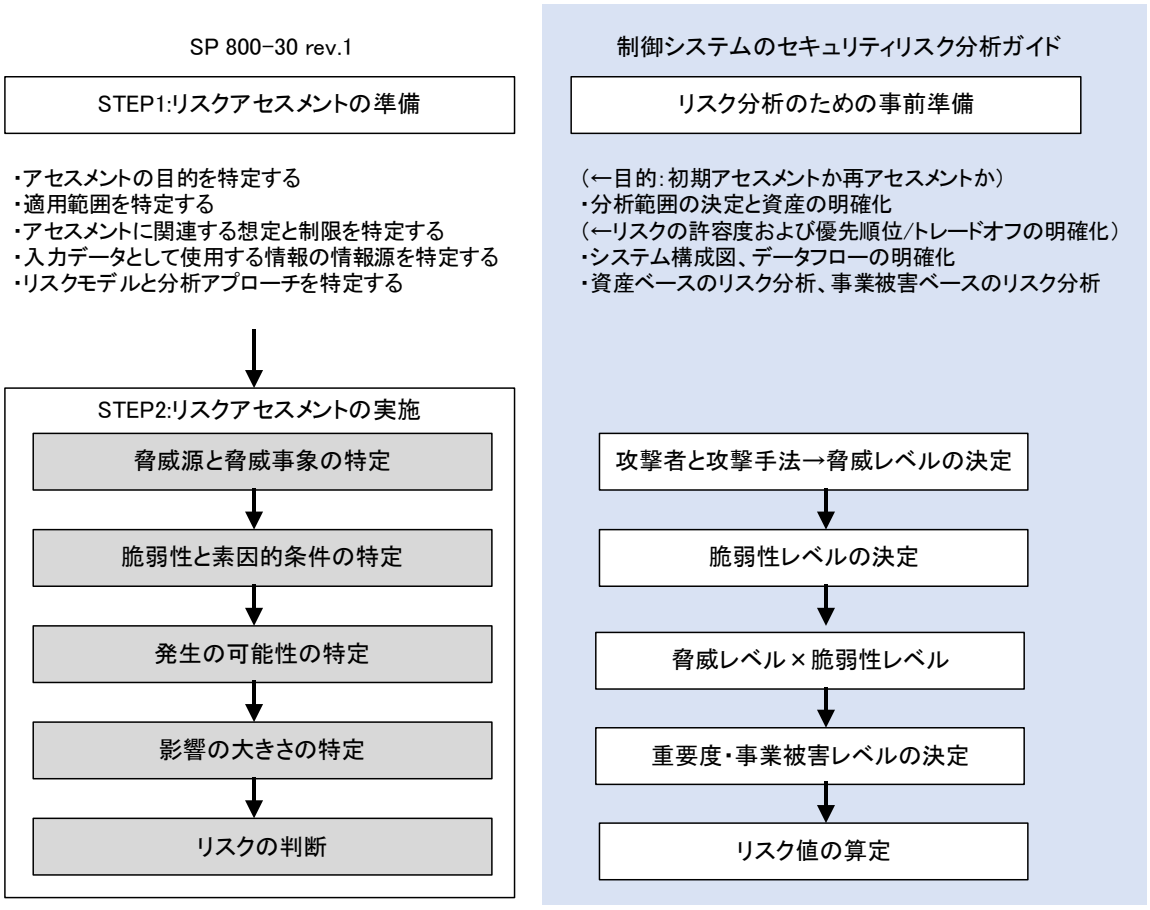

図 9 SP 800-30 リスクアセスメントプロセスとの比較

⑨ ETSI TS 102 165-1 V.5.2.5 (2020-01)と制御システムのセキュリティリスク分析ガイドの分析ステップの比較

ETSI TS 102 165-1 CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) では、リスク分析のプロセスがステップ毎に説明されている。このステップと制御システムのセキュリティリスク分析ガイドの手順を比較したのが図 9 になる。

ETSI の STEP2,3 はリスク分析ガイドでは明示してはいないが、事前準備段階(資産の明確化)で整理を行っている。ETSI の手法に則る場合は、この事前準備段階で STEP2,3 を意識したまとめ方をする事を推奨する。

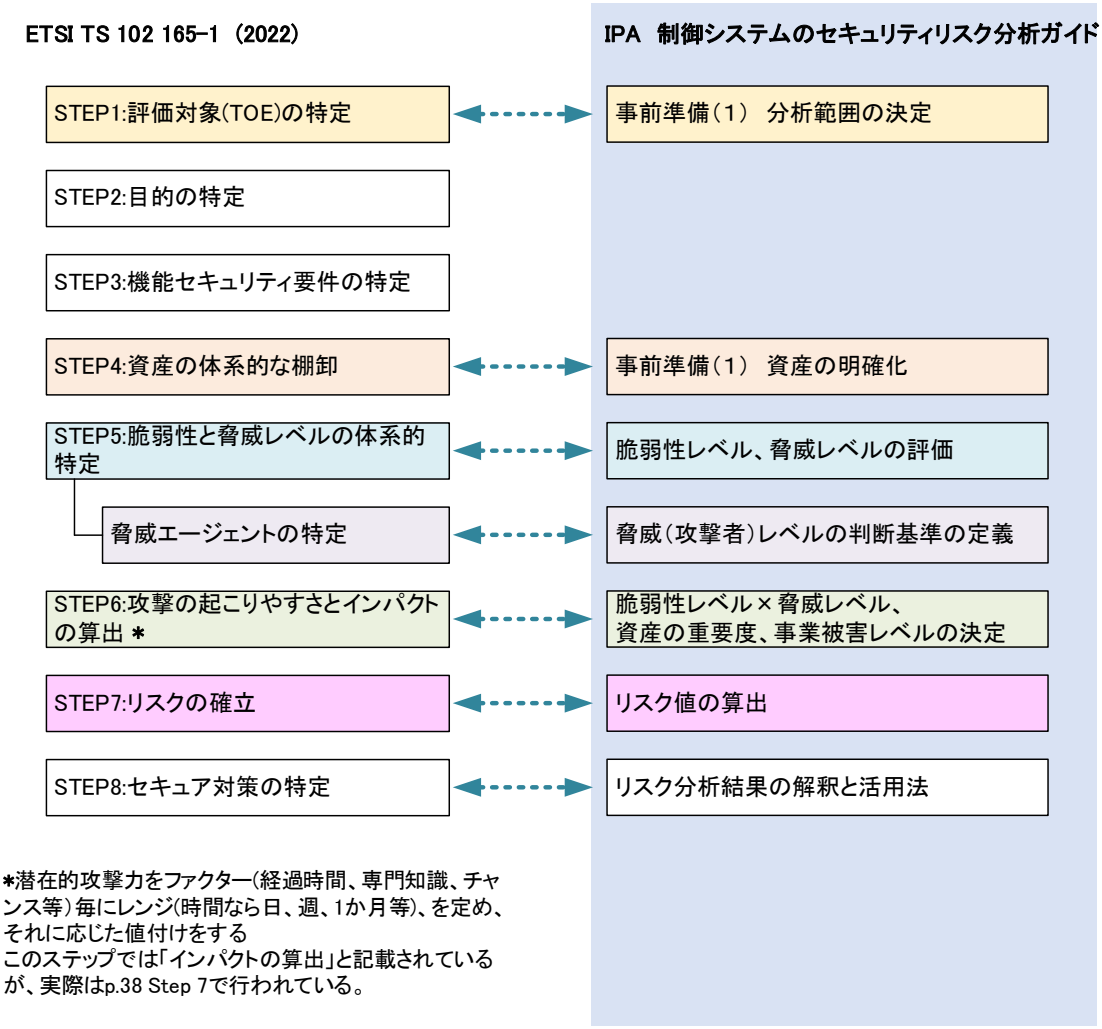

図 10 ETSI TS102-165-1 のプロセスとの比較

5. まとめ

制御システムのセキュリティリスク分析ガイドに記載される詳細リスク分析手法と、リスクアセスメントに言及する国際規格 ISO/IEC 27000 シリーズ、IEC 62443 シリーズや NIST SP 800-30 等との比較を実施し、評価項目の類似性や違いについて明確にした。

- リスク分析ガイドは ISO/IEC 27005:2022 に記述されているリスクアセスメントプロセスの中の[リスク分析]のプロセスだけでなく、[リスク評価]や[リスク特定]、[リスク対応]の一部についてもカバーしている。
- リスク分析ガイドの事業被害ベースのリスク分析で用いられている分析手法である ATA（FTA）、ETA,シナリオベース分析は、IEC 31010:2019 内の分析手法の中で紹介されているものである。
- 分析の範囲という観点では、NIST SP 800-37 に記載されているリスクマネジメントフレームワークの対象が組織と情報システムや運用、教育に対する分析を定義している。一方、リスク分析ガイドでは、制御システムに特化して手法を示している。
- リスク分析ガイドで説明している詳細リスク分析の手順は、資産や、事業被害を生じさせるシナリオを成立させてしまう攻撃ツリーの、脆弱性、脅威のレベルについての評価を行い資産の重要度や事業被害のレベルと組み合わせてリスクの評価を行う、としている。一方、NIST SP 800-30(Rev.1)、IEC 62443-3-2:2020、ETSI TS 102 165-1 V.5.2.5 (2020-01)にも同じ考え方に基づくリスク分析の手順が記されており、これらの手順はリスク分析ガイドと順序は異なるが要素は同じである。また、これらの規格には、手順の詳細な記載はないが、リスク分析ガイドは、分析を実施する際の、より詳細な手引き書となっており、これらの示す手順の具体的な手法に位置付けられる。

以上の様に、IPA の「制御システムのセキュリティリスク分析ガイド」は、主要な国際規格、国際基準に沿った形でリスク分析を行う上で、参考にすることができる詳細リスク分析の手順を記したガイドブックとの認識の下でご利用いただきたい。

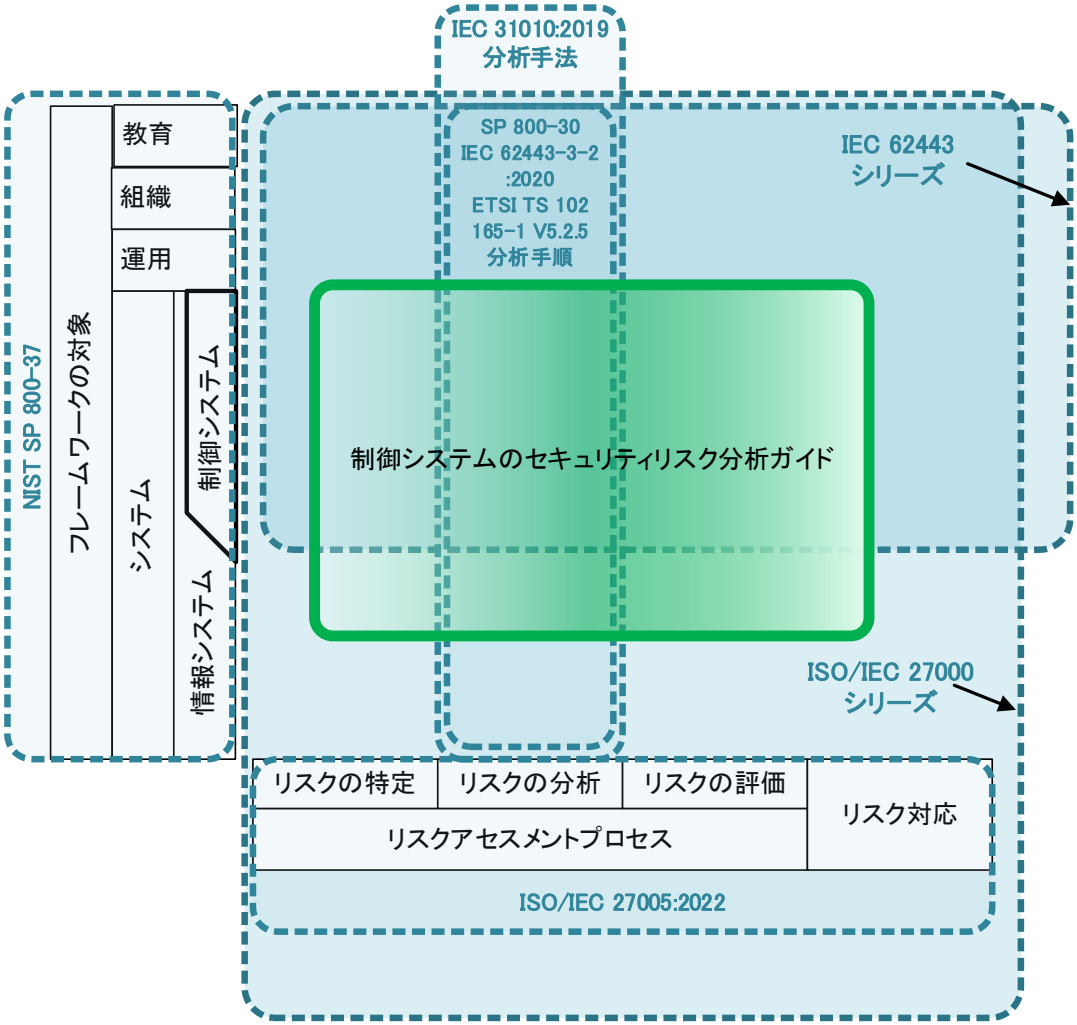

図 11 リスク分析を視点とした国際規格とリスク分析ガイドのスコープ概念図
注：各規格でこの枠組みに正確に沿ったスコープを表現して
いないため、概念図として表現した

６．参考資料

[1] IEC 31010:2019
https://www.iso.org/standard/72140.html

[2] ISO/IEC 27005:2022
https://www.iso.org/standard/80585.html

[3] IEC 62443-2-1 Ed. 2.0:2024 (b)
https://webstore.iec.ch/en/publication/62883

[4] IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design
https://www.en-standard.eu/bs-en-iec-62443-3-2-2020-security-for-industrial-automation-and-control-systems-security-risk-assessment-for-system-design/?gad_source=1&gclid=EAIaIQobChMIqKTB7IykiQMVCeEWBR29BQsaEAMYAiAAEgLo0_D_BwE

[5] NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments
https://csrc.nist.gov/pubs/sp/800/30/r1/final

[6] セキュリティ関連 NIST 文書について
https://www.ipa.go.jp/security/reports/oversea/nist/about.html

[7] NIST SP 800-37 Rev. 2
https://csrc.nist.gov/pubs/sp/800/37/r2/final

[8] ETSI TS 102 165-1 V5.2.5 (2022-01)
https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.05_60/ts_10216501v050205p.pdf

[9] CYBERSECURITY FRAMEWORK
https://www.nist.gov/cyberframework

制御システムのセキュリティリスク分析ガイド補足資料
『制御システムのセキュリティリスク分析ガイド』と国際規格との比較

[著作・制作]　独立行政法人情報処理推進機構　セキュリティセンター
編集責任　辻　宏郷
執筆者　福原　聡