ISA GLOBAL CYBERSECURITY ALLIANCE



ISAGCA ホワイトペーパー

日本の経済安全保障推進法：基幹インフラ制度と ISA/IEC 62443

www.isagca.org

日本の経済安全保障推進法

基幹インフラ制度と ISA/IEC 62443

文書に関する注意事項

本書は、日本の経済安全保障推進法の政策体系を解説し、基幹インフラ制度におけるサイバーセキュリティ関連のリスク管理措置の実施に ISA/IEC 62443 シリーズがどのように寄与できるかを検討するものです法務、法規制対応、調達、エンジニアリング、運用、製品セキュリティ及び産業サイバーセキュリティの各分野に携わる担当者を対象としています。

本書の目的は技術的な情報提供であり、法律上の助言を行うものではありません。

日本語の法律、政令、省令及び告示の原文が正式な根拠となります。英訳及び内閣府の英語資料は、参照と利便性のために提供されています。適用可否は、現行の分野別省令、様式及び届出要領に照らして判断し、必要に応じて所管省庁に確認する必要があります。[1–9]

ISA/IEC 62443 の規格文書は著作権で保護されています。本書は、その適用範囲を要約し分析の根拠として用いていますが、規格の規定文は転載していません。ISA/IEC 62443 への適合、同規格に基づく認証又は評価結果は、それだけで経済安全保障推進法への適合を証明するものではありません。

ISA Global Cybersecurity Alliance（ISAGCA）のために作成：

ShangJyh “SZ” Lin（林上智）
Sun Square Co., Ltd.
最高サイバーセキュリティ顧問

Fukiko Ogura（小倉 福紀）
合同会社 Sun Square Japan
事業開発マネージャー

Copyright © 2026 International Society of Automation. All rights reserved.

目次

要旨 3
目的、適用範囲及び方法 4
1.経済安全保障推進法の政策・法規制の枠組み 5
1.1 政策体系 5
1.2 第 3 章の規制対象範囲 5
1.3 設備導入及び重要維持管理等 6
1.4 届出、審査及び変更 8
1.5 リスク管理措置及びエビデンス 9
2. ISA/IEC 62443 の概要 10
2.1 適用範囲の境界 10
2.2 関連する規格文書 11
2.3 関係者の役割 12
2.4 セキュリティレベルとエビデンスの境界 13
3. 経済安全保障推進法と ISA/IEC 62443 の対応付け 14
3.1 対応付けの方法 14
3.2 サイバーセキュリティのライフサイクル全体にわたる対応関係 14
3.3 内閣府リスク管理措置との詳細な対応付け 15
3.3.1 特定重要設備の導入 16
3.3.2 重要維持管理等の委託 26
3.4 役割とエビデンスの連携 33
4.ギャップと実装上のリスク 34
4.1 ISA/IEC 62443 の適用範囲外となる要求事項 34
4.2 部分的に対応する領域 34
4.3 実装時によく見られる不備 35
4.4 実装上の課題 36
4.5 エビデンスの十分性 37
5. 業界関係者向けガイダンス 38
5.1 アセットオーナー 38
5.2 システムインテグレーター 38
5.3 保守サービスプロバイダー 38
5.4 製品サプライヤー 39
5.5 関係者間の連携 39
6. 結論 41
用語集 42
参考文献 44

要旨

日本の経済安全保障推進法は、特定社会基盤役務の安定的な提供を確保する措置を含め、経済安全保障を強化するための法的措置を定めています。同法第 3 章に基づき、特定社会基盤事業者として指定された事業者は、原則として、特定重要設備を導入する前、又はその重要維持管理等を他社に委託する前に、導入等計画書を事業所管大臣に届け出て、事前審査を受ける必要があります。[1,3–8]

事前審査では、特定重要設備の導入または重要維持管理等の委託に伴い、当該設備が国外から行われる特定妨害行為により特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいかどうかを審査します。[1,3–8]
ISA/IEC 62443 シリーズは、産業用オートメーション及び制御システム（IACS）のサイバーセキュリティを管理するための要求事項とプロセスを規定し、IACS のリスクアセスメント、システムセキュリティ要求事項、安全なインテグレーションと保守、安全な製品開発、脆弱性管理、対策の実施を裏付けるエビデンスの整備を支援します。同規格シリーズは、規制対象となる設備または維持管理の委託に IACS やオートメーションソリューションが関係する場合に、特に高い関連性が高くなります。。対象となる設備の導入や維持管理の委託が、
IACS 環境外の企業 IT、クラウド又は情報処理サービスのみに関係する場合、同規格シリーズの適用はより間接的なものとなります。 [10–21]

経済安全保障推進法は、規制対象となる行為、情報開示、政府による審査及び執行に関する法的拘束力のある義務を定めています。一方 ISA/IEC 62443 は、IACS のセキュリティ管理に関する技術的・組織的要求事項を規定した国際的なサイバーセキュリティ規格シリーズであり、経済安全保障推進法に基づく届出のうちサイバーセキュリティに関する部分を支援できるが、経済安全保障推進法の適用可否を決めるものではなく、法定の届出、企業情報や法域に関する情報開示、事業所管大臣の審査に代わるものではありません。

IACS に関連するケースでは、実務上の対応を進めるにあたり、アセットオーナー、システムインテグレーター、保守サービスプロバイダー、製品サプライヤーなど、関係する各役割の間での連携が必要です。法令上の届出義務を負う主体は特定社会基盤事業者ですが、関連するエビデンスは、システム構成、製品開発記録、コンポーネントのセキュリティ機能、リモートアクセス制御、保守記録及び機密性の高い企業情報などに分散している場合があります。したがって、エビデンスを法規制、製品、システム及び運用に関するものに分類し、それぞれエビデンスの作成、提出及び維持管理に関する責任を明確にする必要があります。

目的、適用範囲及び方法

本書の目的は 3 つあります。第一に、経済安全保障推進法第 3 章の基幹インフラ制度を中心に、同法の政策・法規制の体系を解説します。第二に、特定重要設備の導入及び重要維持管理等の委託に特に関連する ISA/IEC 62443 の部分を要約します。第三に、関係者の役割別に、関連する ISA/IEC 62443 の各規格と経済安全保障推進法のサイバーセキュリティ関連の期待事項との対応関係を整理し、規格の範囲外に残る法的事項、企業情報、サプライチェーン、法域及び継続性に関する事項を明らかにします

本書は、特定社会基盤事業者、関連製品の供給、システムインテグレーション、重要維持管理等、又は IACS 製品の開発・保守を行う組織を対象とし、アセットオーナー、システムインテグレーター、保守サービスプロバイダー、製品サプライヤーという 4 つの機能上の役割に基づいて分析します。これらの役割は分析上の区分であり、経済安全保障推進法が定める法的区分に代わるものではありません。システムインテグレーターと保守サービスプロバイダーーは、ISA/IEC 62443 における広義のサービスプロバイダーのうち異なる業務を担います。また一つの組織が複数の役割を担う場合もあります。製品サプライヤーは、関連する IACS 製品を開発又は保守を行う組織を指します。

法的分析は、2026 年法律第 38 号による改正及び資料の調査基準日現在の施行状況を含む法律に基づいています。施行令、基本指針、適用される分野別省令、内閣府の「特定重要設備の導入版」及び「重要維持管理等の委託版」のパンフレット及び指定事業者の最新一覧も考慮しています。[1–8] 規格の分析には、国際電気標準会議（IEC）が公表する各規格の適用範囲と発行状況に加え、国際自動制御学会（ISA）が示す関係者の役割及び責任の共有に関する説明を使用しています。[10–21]

本書での対応関係の分類は、分析のためのものであり、日本政府、ISA 又は IEC が定めた分類ではありません。分類の定義と適用方法は 3.1 節で説明します。

1. 経済安全保障推進法の政策・法規制の枠組み

1.1 政策体系

国会は 2022 年、安全保障に資する経済施策を総合的かつ一体的に推進するため、経済安全保障推進法を制定しました。同法では、特定重要物資の安定供給、特定社会基盤役務の安定的な提供、特定重要技術の開発支援及び特定の特許出願の非公開に関する制度が設けられました。[1,2,7]

本書では、特定重要設備の導入および重要維持管理等の委託に際し事前の届出と政府による審査を定めていることから、基幹インフラ制度に焦点を当てています。この制度における政策上の懸念は、悪意のあるコードや悪用可能な脆弱性といった技術的なサイバーセキュリティリスクにとどまりません。審査では、特定重要設備の導入又は委託に関連し、当該設備が特定社会基盤役務の安定的な提供に影響する特定妨害行為の手段として使用されるおそれが大きいかどうかを検討します。したがって、サイバーセキュリティは、審査の唯一の対象ではなく、より広範な経済安全保障上の評価の一部として位置づけられます。[3–5]

本書では、2026 年の改正について、第 3 章の制度の適用範囲、施行又は運用に影響する事項に限って扱います。

1.2 第 3 章の規制対象範囲

第 3 章の適用範囲と運用は、複数の法令及び行政文書定められています。法律は対象分野の大枠、主な届出義務及び政府の権限を定めています。政令は、その分野のうち対象となる事業を指定しています。分野別の省令は、指定基準、特定重要設備及び重要維持管理等に該当する業務、必要な届出事項並びに適用されるリスク管理措置を定めています。その上で、事業所管大臣は個々の事業者を特定社会基盤事業者として告示により指定します。基本指針及び内閣府「特定重要設備の導入版」及び「重要維持管理等の委託版」のパンフレットは、政策目的、審査方法及び届出手続を説明していますが、法律、政令又は省令が定める要求事項を変更したり、それらに代わるものではありません。[1,3–5,8]

表 1. 第 3 章に関連する法令及び行政文書

法令・資料	主な役割	実務上の意味・影響
法律	対象分野の大枠、主な届出義務、審査権限、勧告、命令及び継続的な監督を定める。	法的根拠、法的義務及び政府の権限を定める。
政令	法定の対象分野に含まれる事業を具体的に定める。	対象分野の大枠に含まれるだけで、適用が確定するわけではない。
省令	指定基準、特定重要設備及び重要維持管理等に該当する業務、届出事項並びに分野別のリスク管理措置を定める。	適用可否及び届出要件は、該当分野の省令に基づき判断する必要がある。
指定告示	特定社会基盤事業者に指定された個々の事業者を示す。	届出義務は、適用される施行及び経過措置に関する規定に従い、正式に指定された事業者に適用される。
基本指針	政策目的、規制上の原則及び政府の審査方針を説明する。	解釈及び実施の指針となるが、法律、政令又は省令で定められた要求事項を変更するものではない。

法令・資料	主な役割	実務上の意味・影響
内閣府「特定重要設備の導入版」・「重要維持管理等の委託版」のパンフレット	手続についての説明、裏付けとなるエビデンスの例、届出要領及び相談に関する情報を提供する。	届出準備及び制度対応を支援するが、適用される法令や分野別の要求事項に代わるものではない。

2026 年の基幹インフラ制度に関する内閣府資料では、対象事業分野として、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、港湾運送、航空運送、空港、電気通信、放送、郵便、医療、金融及びクレジットカードの 16 分野が示されています。医療は 2026 年の改正で追加されましたが、公布から 18 か月以内に政令で定める日に施行されることとなっていたため、調査基準日時点では、第 3 章の届出制度の運用対象には含まれていませんでした。実際に制度が運用されていたのは 15 分野であり、2026 年 7 月 1 日時点で 258 事業者が特定社会基盤事業者に指定されています。[4–7]

表 2. 2026 年の第 3 章に関する主な改正の施行状況

改正事項	施行規定	2026 年 8 月 14 日時点の施行状況
経過期間中の新規指定事業者による届出	公布から 1 か月後	2026 年 7 月 17 日施行。新たに指定された事業者は、指定後 6 か月の経過期間中に導入等計画書を提出できる。
他の事業者が供給する所定の構成設備を含む、自社供給の特定重要設備	公布から 6 か月以内に政令で定める日	未施行。2026 年 12 月 16 日に施行予定。関連する省令の改正は公布済み。
医療分野の追加	公布から 18 か月以内に政令で定める日	法律には追加済みだが、調査基準日時点では、第 3 章は未施行。

1.3 設備導入及び重要維持管理等

制度の適用可否は、複数の要件をすべて満たすかどうかによります。対象事業が政令で定める範囲に含まれ、事業者が特定社会基盤事業者として正式に指定され、計画されている行為が特定重要設備の導入又は適用される省令で重要維持管理等として定められた業務の委託に該当する必要があります。

設備の導入について、規制対象となるのは特定重要設備であり、適用される省令で、対象となる構成設備が特定されています。これらの設備及びその供給者に関する情報は、該当する届出要件に従って提出する必要があります。システムで使われるその他の部品が、自動的に法定の届出対象となるわけではありません。指定事業者が自ら供給する設備に、他の事業者が供給した所定の構成設備が含まれる場合の取扱いは、関連する 2026 年改正の施行状況に従って判断する必要があります。

導入に関する規制は、法令上の適用除外、経過措置及び緊急時の手続を前提として、指定事業者が他の事業者から供給される特定重要設備を導入しようとする場合に原則として適用されます。法定の届出主体は指定事業者であるが、届け出に必要な情報は設備供給者、所定の構成設備の供給者、関係する場合のシステムインテグレーター、その他導入に関与する当事者が保有している場合があります。必要な情報には、企業情報、議決権の直接保有者、関係役員、製造場所、外国政府又は関連する公的機関との所定の取引、適用されるリスク管理措置のエビデンスなどが含まれる場合があります。[1,3–5,8,23(a)]
重要維持管理等の委託に関する届出制度は、指定事業者が、適用される分野別省令で重要維持管理等と定められた業務を他の事業者に委託する場合に適用されます。

商取引上の呼称だけで適用可否が決まるわけではありません。ベンダー、マネージドサービス事業者、エンジニアリング請負業者又はシステムインテグレーターであっても、実際に行う業務が所定の活動に該当すれば、規制対象の保守管理の委託関係に含まれる可能性があります。一方、広範な商取引又は再委託の関係に含まれているだけで、その組織が第 3 章の情報開示の対象となるわけではありません。[1,3–5,8,23(b)]

重要維持管理等については、原則として、規制対象となる業務を実際に行う事業者まで委託関係に沿って情報の開示が求められます。ただし、下位の再委託先の一部については、適用される省令が定める条件を満たす場合に限り、情報を省略できます。

遠隔地又は海外で業務を行うことだけを理由に、保守管理の委託が第 3 章の適用範囲から除外されることはありません。適用可否は、実際に行う業務が所定の重要維持管理等の定義に該当するかどうかによって判断されます。業務の実施場所や再委託の関係も届出に関係してきます。アクセス対象のシステム及び付与される権限も、業務の性質やサイバーセキュリティリスクの判断に関係する場合があります。[1,3–5,8,23(b)]

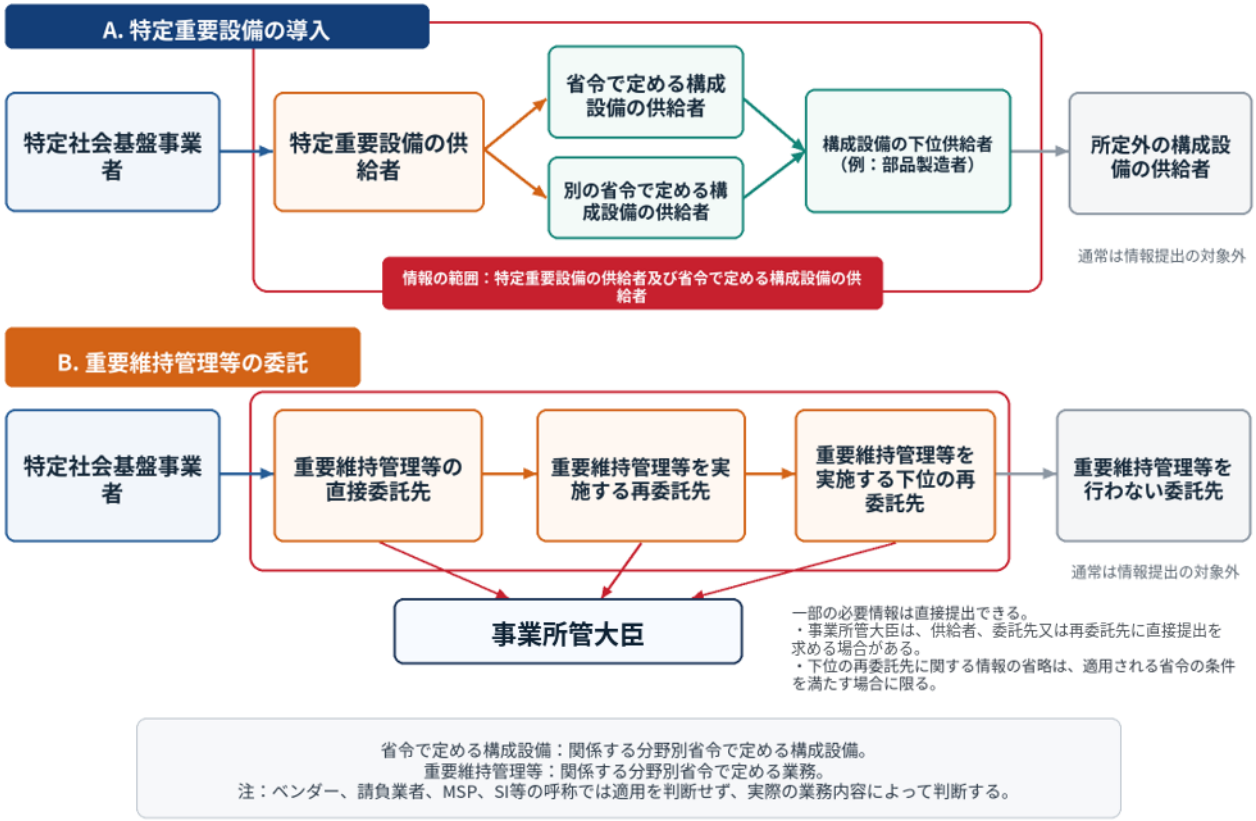

図 1. 経済安全保障推進法に基づくサプライチェーン情報の範囲

出典：内閣府「特定重要設備の導入版」・「重要維持管理等の委託版」のパンフレットを基に筆者が簡略化。特定重要設備の導入と重要維持管理等の委託では、情報開示の考え方が異なる。

1.4 届出、審査及び変更

指定事業者は原則として、規制対象となる行為を開始する前に導入等計画書を提出します。事業所管大臣が計画書を受理すると、通常 30 日間は当該行為の実施が禁止されます。追加審査が不要な場合には期間が短縮され、さらに審査が必要な場合には受理から最長 4 か月まで延長されることがあります。期間の満了又は短縮は、設備や委託関係の認証又は包括的な承認を意味するものではありません。勧告、命令、その他の適用要件に従うことを前提として、法定で定められた実施禁止期間が終了したことを意味します。[1,3–5]

事業所管大臣は、特定重要設備が、その導入又は重要維持管理等の委託に伴い、特定妨害行為の手段として使用されるおそれが大きいと認める場合、事業者に計画の変更、特定妨害行為を防止するため

に必要な措置又は予定する導入・委託の中止を勧告できる。事業者は 10 日以内に勧告を受け入れるかどうかを事業所管大臣に通知し、受け入れない場合には理由を示す必要があります。法定要件を満たす場合には、法的拘束力のある命令が出されることがあります。[1,3–5]

緊急時の手続では、所定の条件を満たす場合に限り、計画書を事前に提出することなく設備の導入又は重要維持管理の委託を進めることができます。これらの条件には、緊急性、事前届出義務を意図的に回避していないこと、特定社会基盤役務の提供に支障が生じることを解消又は防止するために当該導入または委託が必要であること、及び適切な代替手段がないことが含まれます。事業者は導入または委託を実施した後は遅滞なく必要な届出を行わなければなりません。[1,4,5]

導入等計画書の提出後に重要な変更を行う場合は原則として事前の届出が必要となり新たな実施禁止期間が適用されます。その他の法令で定められた変更については遅滞なく届け出る必要がある一方、省令で定める軽微な変更には事前・事後いずれの届出も必要ありません。新たな特定重要設備の導入に該当する変更については、既存の計画書の変更ではなく新たな導入等計画書の提出が必要となります。[1,4,5]

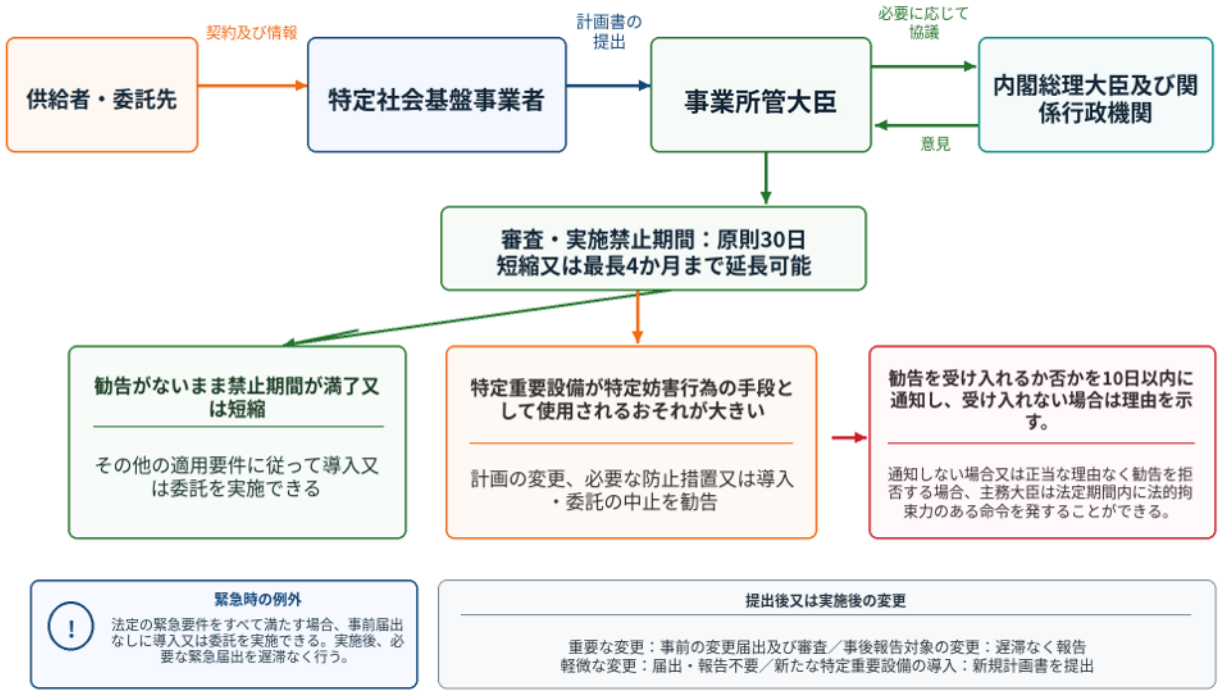

図 2. 経済安全保障推進法のの届出及び政府審査の流れ

出典：内閣府「特定重要設備の導入版」・「重要維持管理等の委託版」のパンフレット及び法定手続を基に、本書向けに要約。

1.5 リスク管理措置及びエビデンス

適用される省令の様式に列挙されたリスク管理措置が、すべての案件で求められるわけではありません。指定事業者は関連するリスクを評価し、その範囲及び程度に応じた措置を講じることが期待されています。導入等計画書には実施した措置を記載し、その実施を裏付ける書類を添付する必要があります。様式に列挙された措置を講じていない場合には、備考欄に同等のリスク管理上の取組を記載することができ、審査において考慮される場合があります。事業所管大臣は、対象となる役務又は事業の状況を踏まえ、措置の実施状況及び事業者によるリスク管理上の取組を評価します。[3–5,8]

内閣府実施資料では、協力が期待される当事者、又は主に措置を講じると想定される当事者に応じてリスク管理措置を分類しています。3.3 節では、これらの措置と関連する ISA/IEC 62443 の各規格文書を詳細に対応付けています。措置の実施を裏付ける資料は契約書やマニュアルに限らず、該当措置の実施を示せるものであれば他の形式も取ることもできます。裏付け資料の十分性は、適用される届出・審査手続において判断されます。

企業の所有関係、議決権の直接保有者、役員に関する情報及び外国政府又は関連する公的機関との特定の取引は、届出及び審査で別途必要となる情報です。これらはサイバーセキュリティ対策ではなく、リスク管理措置が実施されたことを証明するエビデンスとして扱うべきではありません。
[5,8,23(a),23(b)]

供給者、委託先または再委託先に関する情報のうち省令で定められた一部の情報、およびリスク管理措置の実施を裏付ける一部の資料については、指定事業者を経由せず事業所管大臣に直接提出できる場合があります。直接提出の可否は情報・資料の項目ごとに、適用される省令及び様式の記載要領により定められます。直接提出しても、指定事業者が法定の届出主体であることは変わりません。必要な資料がすべて届かなければ届出は受理されず審査も開始されないため、内閣府説明会資料では、主たる計画書を提出する前に、直接提出が必要な資料すべてが所管省庁に到達していることを確認するよう推奨しています。

2. ISA/IEC 62443 の概要

ISA/IEC 62443 規格シリーズは、アセットオーナー、サービスプロバイダー、システム、製品開発およびコンポーネントの各レベルにわたり、産業用オートメーション及び制御システム(IACS)のサイバーセキュリティを扱っています。IACS のサイバーセキュリティの評価と管理に必要な共通概念、役割別の責任及びライフサイクルの要求事項を提供している点で、経済安全保障推進法に関する本書の分析にも関連しています。同規格シリーズは、日本の規制対象となる分野を定義したり、経済安全保障推進法の適用可否を判断したり、届出義務や企業情報開示を定めたり、政府審査に代わったりするものではありません。

2.1 適用範囲の境界

本書における対応付けは、関連する特定重要設備又は省令で定められた構成設備が IACS またはオートメーションソリューションの一部であるか、それらに実質的な影響を及ぼす場合、又は重要維持管理等の委託がそのような IACS またはオートメーションソリューションを対象とする場合に適用されます。デジタル技術、ネットワーク接続又はリモートアクセスが存在するという理由だけで、ISA/IEC 62443 が適切な技術的基盤になるとは限りません。その関連性は、規制対象となる設備又は重要維持管理等の委託における機能、アーキテクチャ、インターフェース及び運用上の依存関係に基づいて評価する必要があります。

経済安全保障推進法の対象となる各分野では、規制対象設備の中に、IACS やオートメーションソリューションを含むものもあれば、企業 IT、クラウド、通信又は分野固有の情報処理システムを主体とするものもあります。対象範囲が IACS の一部ではなく、IACS に実質的な影響も及ぼさない場合は、他のサイバーセキュリティ規格の方が適切な技術的基盤となる可能性があります。これは経済安全保障推進法の適用可否や関連する法定義務を変更するものではありません。ここで用いる境界は本書の分析対象を限定するためのものであり、日本政府、ISA 又は IEC による分類ではありません。

表 3. 技術的状況別の ISA/IEC 62443 の関連性

技術的状況	ISA/IEC 62443 との関連性	主な適用範囲の境界
IACS 又はオートメーションソリューション内のシステムまたはサブシステム	IACS のサイバーセキュリティリスクアセスメント、セキュリティ要求事項、統合、運用及び保守の主要な規格上の根拠となる。	法的な適用可否、届出、企業情報・法域に関する情報及び政府による審査については、別途経済安全保障推進法に基づく分析が必要となる。
検討対象システム（SUC）に含まれるか、IACS とのインターフェースを持つか、IACS に実質的な影響を及ぼす IT・通信・リモートサービスのコンポーネント	定義された IACS の範囲に含まれる場合、その範囲に関連する ISA/IEC 62443 要求事項が適用される。SUC の外部にある場合も、IACS 側のインターフェース、コンジット及び依存関係には関連する。	SUC、ゾーン、コンジット、外部インターフェース及び役割ごとの責任を明確に定義する。外部システム又はサービスには、他のサイバーセキュリティ規格も必要となる場合がある。
SUC に隣接するが、その範囲外にある企業 IT、クラウド又は情報処理システム	ISA/IEC 62443 は IACS 側の境界、アクセス経路及び依存関係を扱えるが、外部システムに対する主要な管理の枠組みではない。	外部システムには別の適切なサイバーセキュリティ規格又は枠組みが必要な場合がある。ISA/IEC 62443 の定義された適用範囲と該当する要求事項を満たさない限り、その一部を適用しただけで規格に適合すると示すべきではない。

技術的状況	ISA/IEC 62443 との関連性	主な適用範囲の境界
IACS に関連する技術的機能を持たない組織・サービス	本書の ISA/IEC 62443 対応付けの範囲外。	経済安全保障推進法上の供給・契約関係に含まれるだけで、ISA/IEC 62443 上の関係者の役割を割り当ててはならない。ただし、同法に基づく情報開示又はデューデリジェンスの要求事項が適用される場合はある。

本表は、IACS 又はオートメーションソリューションと、それに隣接するシステム・サービスの適用範囲を区別しています。経済安全保障推進法に基づく供給関係や委託関係に含まれているという理由だけで、その組織に ISA/IEC 62443 上の関係者の役割を割り当てるべきではありません。適用される役割は、実際に担う機能によって決まります。

2.2 関連する規格文書

本書の対応付けには主に、アセットオーナーのセキュリティプログラム、パッチ管理、インテグレーション及び保守サービス、システムのリスクアセスメントとセキュリティ要求事項、セキュアな製品開発、コンポーネントのセキュリティ機能に関する ISA/IEC 62443 の各規格文書に基づいています。補足的な規格文書は、実装又は評価に関する追加のガイダンスを提供する場合に限り参照しています。

表 4. 本書で参照した主な ISA/IEC 62443 規格

企画	主な適用範囲	本書での用途
IEC 62443-2-1:2024	運用中の IACS に対するアセットオーナーのセキュリティプログラムの方針及び手順の要求事項。	アセットオーナーのガバナンス、運用上のセキュリティプロセス、インシデント対応、継続性及びレガシーIACS に対する補完的措置。
IEC 62443-2-4:2023	オートメーションソリューションの統合・保守を行う IACS サービスプロバイダー向けのセキュリティ関連プロセス要求事項。	システムインテグレーション、保守サービスの提供、要員の力量、管理されたサービス活動及びサービスプロバイダーのセキュリティプロセスに関するエビデンス。
IEC 62443-3-2:2020	SUC、ゾーン及びコンジットの定義、リスクアセスメント、SL-T、文書化されたセキュリティ要求事項を含むシステム設計のセキュリティリスクアセスメント。	システムのリスク分析、セキュリティアーキテクチャーの設計に用いる情報及び文書化されたシステムセキュリティ要求事項。
IEC 62443-3-3:2013	産業用オートメーション及び制御システムのシステムセキュリティ要求事項及びセキュリティレベル。	システムの設計・評価に用いる技術的なシステムセキュリティ要求事項と制御システムのセキュリティ能力レベル。
IEC 62443-4-1:2018	IACS 製品の開発者及び保守担当者に対するセキュアな製品開発ライフサイクル要求事項。	製品セキュリティ要求事項、設計、実装、検証、妥当性確認、欠陥管理、パッチ管理及び製品のサポート終了。
IEC 62443-4-2:2019	IACS コンポーネントの技術的セキュリティ要求事項。	コンポーネントのセキュリティ要求事項及び SL-C（コンポーネント）に関するエビデンス。システム全体の SL-T 又は SL-A を確立するものではない。

IEC PAS 62443-2-2:2025、IEC TS 62443-6-1:2024 及び IEC TS 62443-6-2:2025 は、必要に応じて実装又は評価の補足的ガイドラインとなりますが、経済安全保障推進法との対応付けの主要な根拠ではありません。

IEC 62443-4-1 は製品を開発又は保守する者に適用されます。したがって本書では、対象製品を開発又は保守する組織に限り、IEC 62443-4-1 に関連して製品サプライヤーの役割を割り当てます。機器の販売、流通、組立又は設定だけでは、この役割に該当しません。IEC TR 62443-2-3 は主としてアセットオーナー及び IACS 製品サプライヤーを対象としています。
パッチの評価、展開又はインストール業務をアセットオーナーから契約により委任された場合、保守サービスプロバイダーも同技術報告書の関連部分を適用できます。 [14,18]

2.3 関係者の役割

ISA/IEC 62443 規格シリーズでは、IACS の運用、インテグレーション、保守及び供給を担う組織間で責任を分担するモデルを採用しています。アセットオーナーは IACS を運用し、システムレベルのサイバーセキュリティリスクに関する判断及びセキュリティ要求事項に責任を負います。システムインテグレーターは、その要求事項をオートメーションソリューションの設計、設定、インテグレーション及び検証に反映します。保守サービスプロバイダーは、アクセス制御、変更管理、保守記録及び廃止に関する作業を含む、定められたセキュリティプロセスに従って保守を実施します。製品サプライヤーは対象製品を開発又は保守し、製品のセキュリティ機能、脆弱性管理及びライフサイクル全体に対するサポートを提供します。単一の組織が複数の役割を担う場合も、それぞれの責任及び実施を裏付ける資料は区別されます。

IACS に関係する案件では、アセットオーナーが機能面において特定社会基盤事業者に最も近いですが、この対応関係は機能上のものであり、法的な同一性を意味しません。経済安全保障推進法は、システムインテグレーター、保守サービスプロバイダー又は製品サプライヤーを独立した法定の役割名として用いていません。経済安全保障推進法における組織の位置付けは、実際に行う業務、設備の供給又は保守に関する取引関係上での立場、及び適用される分野別省令によって決まります。

2.4 セキュリティレベルとエビデンスの適用範囲

調達、保証及び規制当局への提出では、セキュリティレベルの用語を慎重に使う必要があります。ISA/IEC 62443-3-2 は、システムのリスクアセスメントを通じて、対象となるゾーン及びコンジットの目標セキュリティレベル（SL-T）を設定します。ISA/IEC 62443-3-3 は、制御システムの技術的要求事項及び対応する能力セキュリティレベル（SL-C（制御システム））を定義し、ISA/IEC 62443-4-2 は、IACS コンポーネントの技術的セキュリティ要求事項と能力セキュリティレベル（SL-C（コンポーネント））を定義しています。

達成セキュリティレベル（SL-A）は、評価対象のシステム範囲で実際に達成されたセキュリティレベルを表し、目標セキュリティレベル及び能力セキュリティレベルのいずれとも異なります。ISA/IEC 62443-4-2 が対象とするのはコンポーネントのセキュリティ能力であり、実装されたシステムが達成したセキュリティレベルではないため、SL-A は同規格の適用範囲外となります。

したがって、コンポーネントの認証又はセキュリティ能力に関する表明だけでは、オートメーションソリューション全体がアセットオーナーの SL-T を満たすことも、特定のシステムレベルの SL-A を達成したことも証明できません。製品及びコンポーネントに関するエビデンスは、システムのリスクアセスメント、構成、統合、設定、検証及び運用に関するエビデンスとあわせて検討する必要があります。

本書では、製品、システム、運用及び法規制に関するのエビデンスを、それぞれ独立したエビデンスの領域として扱います。一つの領域のエビデンスは他の領域の裏付けとなる場合もありますが、それだけで当該エビデンスに定められた範囲を超える保証が得られるわけではありません。製品のエビデンスだけではオートメーションソリューション全体のセキュリティを証明できず、システムの設計・統合に関するエビデンスだけでは運用上の有効性が継続していることを示せるわけではありません。技術的なサイバーセキュリティに関するエビデンスは経済安全保障推進法で求められる企業情報、法域に関する情報又は法規制関連情報に代わるものではありません。

3. ESPA と ISA/IEC 62443 の対応付け

3.1 対応付けの方法

この対応付けでは、第 3 章の期待事項及び内閣府のリスク管理措置のうち、サイバーセキュリティに関係する側面を検討します。経済安全保障推進法の規定と ISA/IEC 62443 の要求事項が法的に同等であると主張するものではありません。各項目について、該当する ISA/IEC 62443 の企画が適切な関係者の役割に適用されるか、関連するサイバーセキュリティ上の目的に対応しているか、実施及び保証に関係する記録またはエビデンスを作成できるかという観点から評価します。講じられた措置及び裏付けとなる書類が個別の設備、維持管理の委託形態及び事業分野について十分であるかどうかは、事業所管大臣が判断します。

表 5. 分析上の対応関係の分類

分類	意味
直接的支援	ISA/IEC 62443 には、経済安全保障推進法の期待事項又は内閣府のリスク管理措置のうちサイバーセキュリティに関係する側面に実質的に対応する、組織、ライフサイクル、サービスプロバイダー又は技術に関する要求事項が含まれる。その実施によって、直接関連する記録や裏付け記録及びエビデンスを得られる場合がある。
部分的支援	ISA/IEC 62443 は、経済安全保障推進法の期待事項又は内閣府のリスク管理措置のうちサイバーセキュリティに関連する重要な部分を扱う。ただし、法的事項、企業情報、サプライチェーン、法域、継続性又はその他の同法固有の事項への対応には追加措置が必要となる。
間接的支援	ISA/IEC 62443 は、経済安全保障推進法の期待事項又は内閣府のリスク管理措置全体を直接扱うものではないが、ガバナンスのプロセス、実施活動又はその結果としてのエビデンスが、評価、実施又は保証を支援できる。
適用範囲外	当該事項は、ISA/IEC 62443 の定義された適用範囲に直接対応するものがない。したがって、適用される経済安全保障推進法上の法的手続、企業・契約・法域・行政上のプロセス、又は適切な場合にはその他の関連する仕組みによって対応する必要がある。

分類は分析上のものであり、経済安全保障推進法の関連する期待事項のうち、サイバーセキュリティの側面に ISA/IEC 62443 がどのように寄与できるかという評価にのみ適用されます。「直接的支援」という評価は、法的な同等性、エビデンスが自動的に認められること又は経済安全保障推進法全体への適合を意味しません。

3.2 サイバーセキュリティのライフサイクル全体にわたる対応関係

経済安全保障推進法のリスク管理措置のうち、サイバーセキュリティガバナンス、システムのリスクアセスメント、セキュリティ要求事項、管理されたインテグレーション及び保守、セキュアな製品開発、脆弱性管理、インシデント対応及び復旧に関係する領域で、ISA/IEC 62443 との対応関係は特に強くなります。これらの領域では、関連する ISA/IEC 62443 規格が、体系化された要求事項、プロセス及び裏付けとなるエビデンスを提供できます。

一方、経済安全保障推進法が企業の所有・支配関係、法域に関連するリスク、外国政府との関係、製造又はサービス提供場所、事業の安定性、供給者又は委託先に関して法令に定められた情報の開示、法定届出及び政府による審査を扱う場合、対応は部分的となるか ISA/IEC 62443 の範囲外となります。ISA/IEC 62443 に関するエビデンスが経済安全保障推進法の手続のうちサイバーセキュリティの部分を裏付ける場合がありますが、これらの事項は適用される法令・法規制の枠組みに基づいて別途

対応する必要があります。

ESPAの対象領域	直接的支援	部分的支援	間接的支援	適用範囲外
サイバーセキュリティのガバナンス	●			
IACSのサイバーセキュリティリスクアセスメント	●			
システムセキュリティ要求事項	●			
セキュアな製品開発	●			
コンポーネントのセキュリティ機能（コンポーネントレベル）	●			
システムインテグレーション及びセキュリティ検証	●			
保守及びリモートアクセスの管理策	●			
脆弱性及びパッチ管理	●			
インシデント対応、バックアップ及び復旧	●			
供給者及び再委託先に関する保証		●		
開発及び製造工程の完全性		●		
製品サポートの継続性及び代替手段		●		
実施状況の証拠			●	
法定の届出及び審査				●
企業の所有及び支配				●
外国政府との関係及び法域上のリスク				●
政府による勧告、命令及び検査				●
国家安全保障及び経済安全保障上の評価				●

注：

● **直接的支援**
ISA/IEC 62443には、該当するESPA領域に対応する要求事項又はプロセスが直接含まれている。

● **部分的支援**
ISA/IEC 62443はESPA領域の一部に対応するが、経済安全保障、法律又は法域に関する事項などには追加措置が必要となる。

● **間接的支援**
ISA/IEC 62443はESPA領域に直接対応しないが、そのプロセス又は証拠は評価、実施及び保証を支援できる。

● **適用範囲外**
ISA/IEC 62443の適用範囲には直接対応する事項がなく、ESPAに関する法的・企業・法域・政府の手続によって対応する。

図 3.経済安全保障推進法と ISA/IEC 62443 の対応関係及びギャップのマトリックス
出典：本書における分析上の対応付け。

次節では、内閣府のリスク管理措置を個別に検討し、ISA/IEC 62443 による直接的、部分的又は間接的な支援が可能な領域と、経済安全保障推進固有の措置が引き続き必要な領域を示します。

3.3 内閣府リスク管理措置との詳細な対応付け

本節では、特定重要設備の導入及び重要維持管理等の委託に関する内閣府のリスク管理措置を、関連する ISA/IEC 62443 の要求事項及びプロセスに対応付けます。複数の実施・協力区分に現れる措置も含め、内閣府の説明会資料と一対一で追跡できるよう、各措置を個別に記載します。措置の表現は内閣府のの概要資料に従い、詳細な説明資料を用いて適用範囲と実施上の位置付けを明確にします。

対応付けは ISA/IEC 62443 がサイバーセキュリティに関連する側面に寄与する部分のみを対象とし、経済安全保障推進法の要求事項との法的同等性を示すものではありません。表 5 で定義した分析上の分類を詳細な対応付け全体を通じて一貫して適用します。実際の届出に適用される措置は、関連する分野別省令及び届出様式に従い、その実施はリスクに応じて行われます。

表 6〜11 の見出しで示す当事者は、ESPA における実施又は協力上の区分であり、ISA/IEC 62443 上の関係者の役割を割り当てたものではありません。これらの表を通じ、適用される導入等計画書の提出及び事業者に求められる確認については、引き続き特定社会基盤事業者が経済安全保障推進法上の責任を負います。供給者、委託先及び再委託先は措置を実施し、又は裏付けとなるエビデンスを提供でき、認められる場合は関連書類の一部を所管事業大臣大臣に直接提出することもできます。IACS に

関係する案件では、特定社会基盤事業者は、機能上、ISA/IEC 62443 のアセットオーナーに最も近いですが、法的又は規範的な同等性を意味しません。ISA/IEC 62443-2-4 では「IACS サービスプロバイダー」を別の意味で用いる。これはインテグレーション又は保守の際に、アセットオーナーにセキュリティ関連プロセスを提供する組織を指します。[5,12,15]

表 8 及び表 11 は主にアセットオーナーの責任を扱っています。表 6 におけるシステムインテグレーション、設置、設定及び検証の活動は、一般に IACS サービスプロバイダーとしてのシステムインテグレーターの役割に対応します。特定重要設備の供給者が関連する IACS 製品を開発又は保守する場合、その範囲には製品サプライヤーの要求事項も適用される可能性があります。表 7 が製品サプライヤーの活動を扱うのは、構成設備の供給者が関連する IACS 製品を開発又は保守する場合に限られます。表 9 及び表 10 が保守サービスプロバイダーの活動を扱うのは、委託先又は再委託先が実際に関連する保守業務を担う場合に限られます。契約上の取引関係における位置付けだけで、ISA/IEC 62443 上の役割が決まるわけではありません。一つの組織が複数の役割を担う場合も、役割ごとの責任及び裏付けとなるエビデンスは区別されます。[5,12,15,18]

表 6、表 7、表 9 及び表 10 における ISA/IEC 62443-2-1 への参照は、アセットオーナーのガバナンス又は監督を支援するものです。表の見出しにある供給者、委託先又は再委託先にアセットオーナーの役割を割り当てるものではありません。ISA/IEC 62443-3-3 及び ISA/IEC 62443-4-2 への参照は、それぞれシステムレベル及びコンポーネントレベルの技術的要求事項を示すものであり、組織上の役割を意味するわけではありません。[12,17,19]

3.3.1 特定重要設備の導入

特定重要設備の導入について、内閣府の資料では、特定重要設備の供給者の協力による措置、構成設備の供給者の協力による措置、特定社会基盤事業者が主に実施する措置に区分しています。特定重要設備の供給者とは、導入予定の対象設備を、その特定重要設備としての機能を備えた状態で製造又は供給する者を指します。特定社会基盤事業者に単に設備を販売する者は含まれず、供給者が必ずしも同事業者の直接の契約相手とは限りません。

同様に、構成設備の供給者とは、適用される省令が定める構成設備を、その機能を備えた状態で製造又は供給する者を指します。特定重要設備の供給者に単に構成設備を販売する者は含まれず、すべての上流の部品供給者に自動的に該当するわけではありません。

措置番号の末尾に「-1」又は「-2」が付く場合、対象となる供給者の位置付けを示します。「-1」は特定重要設備の供給者、「-2」は構成設備の供給者を指します。指定事業者が主に実施する措置という区分は、その主たる実施主体を示しますが、他の関係者の協力を排除するものではありません。これらの経済安全保障推進法上の区分だけで ISA/IEC 62443 上の役割は決まりません。BR は基本要求事項、RE は強化策意味します。SAR、EDR、HDR 及び NDR は、それぞれソフトウェアアプリケーション、組込み機器、ホスト機器及びネットワーク機器の要求事項を指します。その他の接頭辞は、引用した版で用いられる要素識別子に従います。特定重要設備の供給者が関連する IACS 製品の開発又は保守も行う場合、表 7 の対応する構成設備供給者向けの措置に示された ISA/IEC 62443-4-1 の要求事項も適用されます。

表 6. 特定重要設備の導入に関する詳細対応表：特定重要設備の供給者の協力による措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
①-1	(第三者による)受入検査などの検証手順をの構築、脆弱性試験の実施。	**IEC 62443-2-4:2023: SP.02.01 BR; SP.02.02 BR 及び RE(2).** **IEC 62443-3-3:2013:** SR 3.3 及び該当する RE.	直接的支援	経済安全保障推進法上の措置ではこれに加え、指定事業者が導入前の適切な検査及び脆弱性試験の実施体制を確認する必要がある。特定重要設備の供給者又は構成設備の供給者が実施する検査・脆弱性試験は、この措置の対象外となる。
②-1	情報セキュリティ要件（最新のセキュリティパッチや不正プログラム対策ソフトウェアなど）の実装。	**IEC 62443-2-4:2023: SP.10.02 BR; SP.11.01 BR, SP.11.02 BR, SP.11.06 BR.** **IEC 62443-3-3:2013:** SR 3.2.	部分的支援	ISA/IEC 62443 はパッチ管理、悪意のあるコードへの対策及び管理されたサービスプロセスを支援する。経済安全保障推進法ではこれに加え、適用されるセキュリティパッチ及びマルウェア対策の実施状況を含め、契約に定める情報セキュリティ要求事項を供給者が満たしていることを、指定事業者が導入前に設備ごとに確認する必要がある。
③-1	品質保証体制を確立。	**IEC 62443-2-4:2023: SP.02.01 BR.**	部分的支援	IEC 62443-2-4 の SP.02.01 は、オートメーションソリューションのコンポーネントがリスクに応じたセキュリティを備えることを検証する保証プロセスを示す。経済安全保障推進法ではこれに加え、供給者が開発プロセスを含む製造工程について、信頼できる品質保証体制を有することの確認が必要となる。
④-1	開発・製造工程における不正な変更等を定期的又は随時の確認。	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-2-4:2023: SP.06.03 BR.**	部分的支援	経済安全保障推進法ではこれに加え、供給者が開発プロセスを含む製造工程の不正な変更を定期的又は随時確認していることを、指定事業者が確認する必要がある。ISA/IEC 62443 は関連する供給者要求事項及び該当する場合の設定の完全性の検証を支援するが、より広範な製造工程の確認そのものを直接扱うものではない。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑤-1	開発・製造環境への物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）。	**IEC 62443-2-1:2024:** ORG 3.1, USER 1.4, USER 2.1.	部分的支援	IEC 62443-2-1 は、アセットオーナーの IACS セキュリティプログラムにおける物理アクセス管理、アクセス権の割当て及び認可を扱う。経済安全保障推進法ではこれに加え、供給者の開発・製造環境で適切な物理的及び論理的アクセス管理が適用されていることを、指定事業者が確認する必要がある。
⑦	供給者及び導入に携わる者が設備設置時に不正な変更等を防止する体制。	**IEC 62443-2-1:2024:** ORG 1.6, CM 1.4. **IEC 62443-2-4:2023: SP.01.02 RE(1), SP.03.09 BR**	直接的支援	経済安全保障推進法ではこれに加え、特定重要設備の供給者及び導入に関係する他の関係者が、設置時の不正な変更を防ぐために必要な体制を備えていることを、指定事業者が確認する必要がある。
⑧-1	不正な変更のおそれの原因究明体制の担保。	**IEC 62443-2-1:2024:** ORG 1.6, EVENT 1.7, EVENT 1.8. **IEC 62443-2-4:2023: SP.08.01 BR.**	部分的支援	ISA/IEC 62443 は、供給者に対するサイバーセキュリティ要求事項、イベント分析、インシデント調査及び対応を支援する。経済安全保障推進法ではこれに加え、導入後に不正な変更が発見又は疑われた場合、供給者が詳細調査及び現地検査に協力することを指定事業者が確認する必要がある。
⑨-1	供給者によるサービス保障（故障対応や脆弱性対応等）。	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-2-4:2023: SP.03.03 BR; SP.11.01–SP.11.06 BR.**	部分的支援	ISA/IEC 62443 は、供給者のライフサイクルサポート要求事項、脆弱性管理及びセキュリティパッチの提供を支援する。経済安全保障推進法ではこれに加え、故障及び脆弱性への対応を含む十分なアフターサービスを供給者が保証することを、指定事業者が確認する必要がある。より広範なアフターサービスやサイバーセキュリティに関連しない故障対応は、ISA/IEC 62443 の定義された適用範囲外となる。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑩-1	サービス保障が受けられなくなった場合の代替手段の検討。	**IEC 62443-2-1:2024:** ORG 1.6, COMP 3.5, AVAIL 1.1, AVAIL 1.2. **IEC 62443-2-4:2023: SP.11.02 RE(2).**	部分的支援	ISA/IEC 62443 は事業継続性計画及び、該当する場合には通常の脆弱性是正措置が適用できない際の緩和措置を支援する。経済安全保障推進法ではこれに加え、供給者によるアフターサービス自体が利用できなくなる可能性を踏まえ、代替手段又はその他の必要な対応を指定事業者が検討する必要がある。
⑬	設備に対するアクセスの制御及び不正アクセスの監視の仕組みの実装。	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023: SP.03.07 BR, SP.08.02 BR. IEC 62443-3-3:2013:** SR 1.1, SR 1.2, SR 2.1, SR 2.8, SR 6.2.	直接的支援	経済安全保障推進法ではこれに加え、指定事業者自身又は特定重要設備の供給者が、必要なアクセス制御及び不正アクセス監視機能を実装することを、指定事業者が導入前に確認する必要がある。
⑭-1	過去 3 年間の国内関連法規・国際的な基準の違反の確認	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	経済安全保障推進法は、届出前 3 年間の遵守状況を含め、供給者が適用される国内法令を遵守及び国際規格に適合していることの確認を指定事業者に求める。この法令・規制の遵守履歴の確認は ISA/IEC 62443 の適用範囲外である。
⑮-1	外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	経済安全保障推進法は、外国の法令又は外部の主体からの明示・黙示の指示によって契約違反が生じる可能性がある場合について、その旨を報告する義務を契約上定めることを指定事業者に求める。この法的事項及び外国からの影響に関する報告要件は ISA/IEC 62443 の適用範囲外である。
⑰	供給者に関する詳細情報提供の担保	**IEC 62443-2-1:2024:** ORG 1.5, ORG 1.6.	間接的支援	ISA/IEC 62443 は、供給者へのサイバーセキュリティ要求事項及び IACS に関わる要員のサイバーセキュリティの力量・教育要件を支援する。経済安全保障推進法ではこれに加え、企業の識別情報、所在地、役員、資本関係、事業情報、製造場所、関係する要員の情報、及びこれらの変更が生じた場合の適時の通知を含む、より広範な供給者の情報が求められる。

表 7. 特定重要設備の導入に関する詳細対応表：構成設備の供給者の協力による措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
①-2	(第三者による)受入検査等の検証体制の構築、脆弱性検査の実施	**IEC 62443-2-4:2023:** SP.02.01 BR; SP.02.02 BR 及び RE(2).	直接的支援	ISA/IEC 62443-2-4 は、導入前の構成設備について、サービスプロバイダーが実施する検査及び脆弱性試験の体制を直接支援する。指定事業者は、関連する構成設備がその体制の対象に含まれることを確認しなければならない。この確認は特定重要設備の供給者を通じて行うことができる。各構成設備の供給者自身が実施する試験は、この経済安全保障推進上の措置の対象から除外される。供給者が実施する IEC 62443-4-1 の SVV-3 の試験は製品の保証を支援し得るが、それだけでこの措置の要求満たすわけではない。
②-2	情報セキュリティ要件（最新のセキュリティパッチや不正プログラム対策対策ソフト等）の実施	**IEC 62443-4-1:2018: SUM-1, SUM-4, SUM-5. IEC 62443-4-2:2019: 該当する SAR/EDR/HDR/NDR 3.2; 該当する EDR/HDR/NDR 3.10 及び RE(1).**	部分的支援	ISA/IEC 62443-4-1 及び ISA/IEC 62443-4-2 は、セキュリティ更新プロセス、更新機能及び悪意のあるコードへの対策を支援するが、導入前に最新の適用可能なセキュリティパッチやマルウェア対策の更新が構成設備に適用済みであることを保証するものではない。経済安全保障推進法ではこれに加え、契約時に定めた情報セキュリティ要求事項が満たされていることを指定事業者が確認する必要がある。この確認は特定重要設備の供給者を通じて行うことができる。
③-2	品質保証体制の確立	**IEC 62443-4-1:2018: SM-1, SM-12, SM-13.**	部分的支援	ISA/IEC 62443-4-1 は、セキュア開発プロセスのガバナンス、プロセスの検証及び継続的改善を扱う。経済安全保障推進法ではこれに加え、開発プロセスを含む製造工程全体の品質保証体制を対象とする。
④-2	開発・製造過程における不正な変更等を定期的又は随時の確認	**IEC 62443-2-1:2024: ORG 1.6, ORG 2.3. IEC 62443-4-1:2018: SM-1, SM-7.**	部分的支援	経済安全保障推進法では、関連する各構成設備供給者が、開発プロセスを含む製造工程の不正な変更を定期的又は必要に応じて確認していることの確認が必要となる。ISA/IEC 62443 は、関連するサプライチェーン管理及びセキュア開発の完全性に関する管理策を提供するが、製造工程全般の確認は経済安全保障推進法固有の措置である。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑤-2	開発・製造環境への物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）	**IEC 62443-2-1:2024: ORG 1.6.** **IEC 62443-4-1:2018: SM-7.**	部分的支援	ISA/IEC 62443 はサプライチェーンのセキュリティ要求事項及び、該当する場合の製品開発環境の保護を支援する。ESPA ではこれに加え、開発環境を含む関連する製造環境全体で、適切な物理的及び論理的アクセス管理が行われていることの確認が必要となる。
⑧-2	不正な変更のおそれの原因究明体制の担保	**IEC 62443-2-1:2024:** ORG 1.6, EVENT 1.7, EVENT 1.8. **IEC 62443-4-1:2018: DM-1, DM-2, DM-3.**	部分的支援	ISA/IEC 62443 は、供給者へのサイバーセキュリティ要求事項及び、該当する場合の製品セキュリティ上の問題の調査や根本原因分析を支援する。経済安全保障推進法ではこれに加え、導入後に不正な変更が発見又は疑われた場合に、構成設備供給者が詳細調査及び現地検査に協力することの確認が必要となる。
⑨-2	供給者によるサービス保障（故障対応や脆弱性対応等）	**IEC 62443-2-1:2024: ORG 1.6, ORG 2.3.** **IEC 62443-4-1:2018: DM-1–DM-5; SUM-1–SUM-5.**	部分的支援	ISA/IEC 62443 は、供給者に対するライフサイクルサポート要求事項及び、該当する場合の製品の脆弱性の取扱い、是正、情報開示並びにセキュリティ更新の提供を支援する。経済安全保障推進法ではこれに加え、故障や脆弱性への対応を含む十分なアフターサービスを構成設備供給者が保証することの確認が必要となる。より広範なアフターサービス及びサイバーセキュリティに関連しない故障対応は、ISA/IEC 62443 の定義された範囲外となる。
⑩-2	サービス保障が受けられなくなった場合の代替手段の検討	**IEC 62443-2-1:2024: ORG 1.6, COMP 3.5, AVAIL 1.1, AVAIL 1.2.** **IEC 62443-4-1:2018: DM-4, SUM-2, SUM-5**	部分的支援	ISA/IEC 62443 は継続性計画及び、セキュリティパッチを展開できない際の補完的な緩和措置を含む、代替的な脆弱性対応を必要に応じて支援する。経済安全保障推進法ではこれに加え、供給者によるアフターサービス自体が利用できなくなる可能性を踏まえ、代替手段又はその他の必要な対応を指定事業者が検討する必要がある。
⑭-2	過去 3 年間の国内関連法規・国際的な基準の違反の確認	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	ESPA では、関連する各構成設備供給者について、届出前 3 年間の遵守状況を含め、適用される国内法令の遵守及び国際規格への適合していることの確認を求める。この法令・規制の遵守履歴の確認は ISA/IEC 62443 の適用範囲外である。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑮-2	外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	経済安全保障推進法は、外国の法令又は外部の主体からの明示・黙示の指示によって契約違反が生じる可能性がある場合について、その旨を報告する義務を契約上定めることを指定事業者に求める。この法的事項及び外国からの影響に関する報告要件は ISA/IEC 62443 の適用範囲外である。
⑰	供給者に関する詳細情報提供の確保	**IEC 62443-2-1:2024: ORG 1.5, ORG 1.6. IEC 62443-4-1:2018: SM-2, SM-4.**	間接的支援	ISA/IEC 62443 は、供給者へのサイバーセキュリティ要求事項及び IACS に関わる要員のサイバーセキュリティの力量・教育要件を支援する。経済安全保障推進法ではこれに加え、企業の識別情報、所在地、役員、資本関係、事業情報、製造場所、関係する要員の情報、及びこれらの変更が生じた場合の適時の通知を含む、より広範な供給者の情報が求められる

表 8. 特定重要設備の導入に関する詳細対応表：主に特定社会基盤事業者が実施する措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	ESPA 固有の追加検討事項
①	(第三者による)受入検査等の検証体制の構築、脆弱性検査の実施	**IEC 62443-2-1:2024:** ORG 2.2. **IEC 62443-2-4:2023:** SP.02.01 BR; SP.02.02 BR 及び RE(2). **IEC 62443-3-3:2013:** SR 3.3 及び該当する RE.	部分的支援	ISA/IEC 62443 は、脆弱性その他のセキュリティ上の異常の検出、オートメーションソリューションのセキュリティ試験、及びコンポーネントがリスクに応じたセキュリティを備えることのエビデンスを支援する。経済安全保障推進法上の措置ではこれに加え、指定事業者が導入前の適切な検査及び脆弱性試験の実施体制を確認する必要がある。特定重要設備の供給者又は構成設備の供給者が実施する検査・脆弱性試験は、この措置の対象外となる。
⑥	インターネット接続時の不正アクセス防止機能実装、マニュアル整備	**IEC 62443-2-1:2024:** NET 1.1, NET 1.7. **IEC 62443-3-3:2013:** SR 1.13, SR 5.2.	直接的支援	経済安全保障推進法は、特定重要設備をインターネットに接続する場合に、指定事業者がこれらの管理策を適用し、関連するマニュアル及び指針を整備して遵守することを求める。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	ESPA 固有の追加検討事項
⑩	サービス保障がが受けられなくなった場合の代替手段の検討	**IEC 62443-2-1:2024:** ORG 1.6, AVAIL 1.1, AVAIL 1.2.	部分的支援	ISA/IEC 62443 は、アセットオーナーのサプライチェーン及び運用継続性の計画を支援する。ESPA は特に、供給者のサービスが利用できなくなる可能性に備え、代替手段その他の必要な対応を含めて緊急時の対応を計画するよう求める。
⑪	不正な妨害が行われた場合でも役務の提供を継続できる体制の整備	**IEC 62443-2-1:2024: AVAIL 1.1, AVAIL 1.2, AVAIL 2.1, AVAIL 2.3, AVAIL 2.4, AVAIL 2.5. IEC 62443-3-3:2013: SR 7.3, SR 7.4.**	直接的支援	ESPA では、これらの継続・復旧の体制を、障害発生時にも特定社会基盤役務を継続して提供するために適用し、対策の一例として特定重要設備を代替設備に置き換えることを明示している。
⑫	インシデント発生時の対応方針及や体制の整備	**IEC 62443-2-1:2024:** EVENT 1.7, EVENT 1.8.	直接的支援	ESPA は、指定事業者がインシデント対応方針及び体制を維持することを求め、文書化されたマニュアル及び定期的なインシデント対応訓練を実施例として示している。
⑬	不正なアクセスの制御及び監視の仕組みの実装	**IEC 62443-2-1:2024:** USER 2.1, EVENT 1.1, EVENT 1.4. IEC 62443-3-3:2013: SR 1.1, SR 1.2, SR 2.1, SR 2.8, SR 6.2.	直接的支援	経済安全保障推進法ではこれに加え、指定事業者自身が、必要なアクセス制御及び不正アクセス監視機能を実装することを、指定事業者が導入前に確認する必要がある。
⑯	映像機器の情報の取扱いの適切性確認（特定重要設備の設置場所）	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	監視カメラやドローンなどの映像取得機器が、特定重要設備を設置又は使用する場所に設置・使用される場合、経済安全保障推進法は、機器供給者の本店所在地の法的環境によって映像情報の取扱いの適切性が影響を受けないことを、指定事業者に確認するよう求める。この確認には、供給者の議決権の過半数を直接又は間接に保有する者の所在地の法的環境も含まれる。こうした法的環境の評価は ISA/IEC 62443 の適用範囲外である。

3.3.2 重要維持管理等の委託

重要維持管理等の委託について、内閣府の資料では、委託先の協力による措置、再委託先の協力による措置、特定社会基盤事業者が主に実施する措置に区分しています。同じ措置が複数の区分に現れる場合があるのは、実施、確認又は裏付けとなるエビデンスの提供に、委託関係上の異なる当事者が関与するためです。

一部の措置については、委託先が再委託先の実施状況を確認できます。ただし、これにより委託先と再委託先が同じ役割になるわけではありません。委託先及び再委託先は経済安全保障推進法上の契約関係での位置付けであり、実際に該当する保守サービス業務を行う組織に限り、ISA/IEC 62443 の保守サービスプロバイダーの役割に対応付けるべきです。

表 9. 重要維持管理等の委託に関する詳細対応表：委託先の協力による措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
①	操作ログや作業履歴等の保管や不正な変更の有無の定期的又は随時の確認	**IEC 62443-2-4:2023:** SP.01.02 RE(1), SP.03.10 RE(2), SP.06.01 RE(1), SP.06.03 BR, SP.08.02 BR 及び RE(2), SP.08.03 BR.	直接的支援	内閣府の説明会資料ではさらに、委託先の手順において、作業を実施した者又は機器と正確な日時を記録し、収集する操作ログ・作業履歴と 1 年以上の保存期間を定め、記録を不正な削除・改変・アクセスから保護し、その記録を使って不正な操作又は変更の有無を定期的又は随時に確認することを示している。したがって、対象設備に固有の保存記録が引き続き必要であり、サービスプロバイダーの手順書や認証だけでは、対象となる保守作業が実施されたことを証明できない。
③	保有している設計書や設備等の情報への物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）	**IEC 62443-2-4:2023:** SP.01.03 BR, SP.03.10 BR, SP.03.10 RE(1).	部分的支援	ISA/IEC 62443 は、アセットオーナーの機密情報の保護と機微情報への論理的アクセス管理を支援する。経済安全保障推進法ではこれに加え、委託先が保有する関連する設計仕様書及び設備情報に対し、適切な物理的・論理的アクセス管理を適用することを求めている。
④	実施環境における物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）	**IEC 62443-2-4:2023:** SP.01.02 BR, SP.01.02 RE(1), SP.01.07 BR, SP.03.07 BR, SP.09.01 BR, SP.09.02 BR, SP.09.04 BR.	部分的支援	ISA/IEC 62443 は、保守・エンジニアリング業務に関わる要員のセキュリティ要求事項及び論理的アクセス管理を支援する。経済安全保障推進法ではこれに加え、委託業務を実施する環境全体で適切な物理的・論理的アクセス管理を求めている。
⑤	サイバーセキュリティ教育	**IEC 62443-2-4:2023:** SP.01.01 BR, SP.01.02 BR.	部分的支援	ISA/IEC 62443 は、関係するサービスプロバイダーの要員が、適用されるサイバーセキュリティ要求事項、責任、方針及び手順を認識し、遵守することを求める。内閣府の説明会資料ではさらに、重要維持管理等を実施又は支援するすべての要員及び責任者に対し、各事業年度に少なくとも 1 回のサイバーセキュリティ教育を実施することを示している。
⑥	再委託を行う場合における、特定社会基盤事業者の承認等	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1).	間接的支援	ISA/IEC 62443 はサプライチェーンのセキュリティ要求事項及び再委託先要員のセキュリティ要求事項を支援するが、委託先が再委託の都度、指定事業者の事前承認を得ることまでは求めていない。
⑦	再委託先を行う場合の委託先と同等のサイバーセキュリティ対策の確保	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.02 BR, SP.02.03 RE(1).	部分的支援	ISA/IEC 62443 は、再委託先まで連鎖するサプライチェーンのサイバーセキュリティ要求事項及び再委託先の要員への関連する要求事項・手順の適用を支援する。経済安全保障推進法ではこれに加え、すべての再委託階層において、委託先が自らと同等のサイバーセキュリティ対策を確保することを求める。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑧	事業計画等による事業の安定性の確認	**ISA/IEC 62443 に直接対応する事項なし。**	適用範囲外	経済安全保障推進法は、事業計画、財務の健全性及びサービス提供実績などに基づき、委託先と関係する各再委託先の事業の安定性を確認することを求める。この事業・財務面のデューデリジェンス評価は ISA/IEC 62443 の適用範囲外である。
⑨-1	過去 3 年間の国内関連法規及び国際的な基準の違反の確認	**ISA/IEC 62443 に直接対応する事項なし。**	適用範囲外	経済安全保障推進法は、届出前 3 年間の遵守履歴を含め、委託先が適用される国内法令の遵守及び国際規格の適合していることの確認を求める。この法令・規制の遵守履歴の確認は ISA/IEC 62443 の適用範囲外である。
⑩-1	外国の法的環境等による契約違反が生じたおそれがある場合の報告義務る。	**ISA/IEC 62443 に直接対応する事項なし。**	適用範囲外	ESPA は、外国の法的環境又は外部の主体からの明示・黙示の指示により、指定事業者との契約に違反する行為が生じた可能性がある場合、委託先が指定事業者に直ちに報告することを契約上義務付けるよう求める。この法的事項及び外国からの影響に関する報告条件は ISA/IEC 62443 の適用範囲外である。
⑫	供給者に関する詳細な情報提供の確保	**IEC 62443-2-1:2024:** ORG 1.3, ORG 1.6. **IEC 62443-2-4:2023:** SP.01.05 BR, SP.01.06 BR, SP.01.07 BR.	間接的支援	ISA/IEC 62443 は、役割、セキュリティ担当窓口、要員資格及び担当要員の変更に関するセキュリティ関連情報の提供を支援できる。経済安全保障推進法ではこれに加え、委託先及び関係する再委託先の名称・所在地、役員及び所有関係、事業計画及び実績、重要維持管理等の実施場所、関係要員の所属及び専門性について、これらの情報の提供及び契約締結後の変更に関する適時の通知を、契約上確保することが求められる。

表 10. 重要維持管理等の委託に関する詳細対応表：再委託先の協力による措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
①	操作ログや作業履歴等の保管や不正な変更の定期的又は随時の確認	**IEC 62443-2-4:2023:** SP.01.02 RE(1), SP.03.10 RE(2), SP.06.01 RE(1), SP.06.03 BR, SP.08.02 BR 及び RE(2), SP.08.03 BR.	直接的支援	内閣府の説明会資料ではさらに、委託先の手順において、作業を実施した者又は機器と正確な日時を記録し、収集する操作ログ・作業履歴と 1 年以上の保存期間を定め、記録を不正な削除・改変・アクセスから保護し、その記録を使って不正な操作又は変更の有無を定期的又は随時に確認することを示している。したがって、対象設備に固有の保存記録が引き続き必要であり、サービスプロバイダーの手順書や認証だけでは、対象となる保守作業が実施されたことを証明できない。
③	保有している設計書・設備等の情報への物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）	**IEC 62443-2-4:2023:** SP.01.03 RE(1), SP.03.10 BR, SP.03.10 RE(1).	部分的支援	ISA/IEC 62443 は、再委託先要員の秘密保持義務及び機微情報の論理的保護を支援する。経済安全保障推進法ではこれに加え、関係する各再委託先が保有する設計仕様書及び設備情報について、適切な物理的・論理的アクセス管理を適用することを求めている。
④	実施環境における物理的（入退室管理）及び論理的な制御（システムへのアクセス制御）	**IEC 62443-2-4:2023:** SP.01.01 RE(1); SP.01.02 BR 及び RE(1); SP.01.07 BR; SP.03.07 BR; SP.09.01 BR; SP.09.02 BR; SP.09.04 BR.	部分的支援	ISA/IEC 62443 は、再委託先要員のセキュリティ要求事項及びアクセス関連の管理策を支援する。ESPA ではこれに加え、関係する各再委託先が、委託業務を実施する環境全体で適切な物理的・論理的アクセス管理を適用することを求めている。
⑤	サイバーセキュリティ教育	**IEC 62443-2-4:2023: SP.01.01 RE(1), SP.01.02 BR.**	部分的支援	ISA/IEC 62443 は、関係する再委託先の要員が、適用されるサイバーセキュリティ要求事項、責任、方針及び手順を認識し、遵守することを求める。内閣府の説明会資料ではさらに、重要維持管理等を実施又は支援するすべての要員及び責任者について、各事業年度に少なくとも 1 回の教育を実施することを示している。新たに担当となった要員は、後日の実施に合理的な理由がある場合を除き、配属から 3 か月以内に教育を修了すべきであり、参加・理解状況を記録して教育内容を最新に保つべきである。
⑥	再委託を行う場合における特定社会基盤事業者の承認等	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1).	間接的支援	ISA/IEC 62443 は、再委託先まで連鎖するサプライチェーンのセキュリティ要求事項及び再委託先要員に対するセキュリティ要求事項を支援するが、再委託先がさらに委託する前に指定事業者の事前承認を得ることまでは求めていない。
⑦	再委託先を行う場合の委託先と同等のサイバーセキュリティ対策の確保	**IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.02 BR, SP.02.03 RE(1).	部分的支援	ISA/IEC 62443 は、再委託先の要員及び活動への関連するサイバーセキュリティ要求事項・手順の適用を支援する。経済安全保障推進法ではこれに加え、その先のすべての再委託階層で、委託先と同等のサイバーセキュリティ対策を確保することを求める。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑨-2	過去 3 年間の国内関連法規及び国際的な基準の違反の確認	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	経済安全保障推進法は、関係する各再委託先について、届出前 3 年間の遵守履歴を含め、適用される国内法令の遵守及び国際規格への適合していることの確認を求める。この法令・規制の遵守履歴の確認は ISA/IEC 62443 の適用範囲外である。
⑩-2	外国の法的環境等による契約違反が生じたおそれがある場合の報告義務	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	経済安全保障推進法は、外国の法的環境又は外部の主体からの明示・黙示の指示により、該当する契約に違反する行為が生じた可能性がある場合、指定事業者又は再委託を行った者に直ちに報告することを、該当する再委託契約において義務付けるよう求める。 この法的事項及び外国からの影響に関する報告条件は、ISA/IEC 62443 の適用範囲外である。
⑫	供給者に関する詳細な情報提供の確保	**IEC 62443-2-1:2024:** ORG 1.3, ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.07 BR.	間接的支援	ISA/IEC 62443 は、再委託先の要員及び担当要員の変更に関する限定的なセキュリティ関連情報を提供する。経済安全保障推進法ではこれに加え、関係する各再委託先の名称・所在地、役員及び資本関係、事業計画及び実績、業務の実施場所、関係要員の所属及び専門性について、これらの情報の提供及び契約締結後の変更に関する適時の通知を、契約上確保することを求める。

表 11. 重要維持管理等の委託に関する詳細対応表：主に特定社会基盤事業者が実施する措置

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
②	最新のセキュリティパッチ適用等の定期的な資産管理	**IEC 62443-2-1:2024:** CM 1.1, COMP 3.2, COMP 3.3, COMP 3.5.	直接的支援	内閣府の説明会資料は、指定事業者に対し、特定重要設備とその構成設備の状態を定期的に管理し、最新の適用可能なセキュリティパッチが適用されているか確認するとともに、代替予定の設備についても同等の定期的な資産管理を行うことを求めている。そのため、指定事業者には設備ごとの最新の資産台帳とパッチ適用状況の証拠が必要となる。製品サプライヤーのパッチ情報だけでは実際の適用状況は示せず、未適用のパッチがある場合には、設備ごとのリスク対応を文書化する必要がある。
⑥	再委託を行う場合における特定社会基盤事業者の承認等	**IEC 62443-2-1:2024:** ORG 1.6.	間接的支援	内閣府の説明会資料は、委託先による再委託及びさらに下位の再委託について、指定事業者の事前承認を条件とすることを契約又は同等の取決めで確保するよう求めている。ISA/IEC 62443 はアセットオーナーのサプライチェーンガバナンスを支援するが、この経済安全保障推進法固有の事前承認条件を定めていない。
⑧	事業計画等による事業の安定性の確認	ISA/IEC 62443 に直接対応する事項なし。	適用範囲	ESPA は、指定事業者が委託先及び関係する再委託先の事業の安定性を評価・確認することを求めている。ISA/IEC 62443 は、事業計画、財務の健全性又は事業全体の継続可能性を評価する要求事項を定めていない。

届出様式の措置番号	内閣府のリスク管理措置	関連する ISA/IEC 62443 の支援	評価	経済安全保障推進法固有の追加検討事項
⑪	映像機器の情報の取扱いの適切性確認（重要維持管理等の場所）	ISA/IEC 62443 に直接対応する事項なし。	適用範囲外	監視カメラやドローンなどの映像取得機器が、重要維持管理等を実施する場所に設置又は使用される場合、経済安全保障推進法は、機器供給者の本店所在地の法的環境によって映像情報の取扱いの適切性が影響を受けないことを、指定事業者に確認するよう求める。この確認には、供給者の議決権の過半数を直接又は間接に保有する者の所在地の法的環境も含まれる。こうした法域及び法的環境の評価は、ISA/IEC 62443 の適用範囲外である。

3.4 役割とエビデンスの連携

法定の届出主体は指定事業者であり、実務上は複数の組織が保有する情報及びエビデンスを取りまとめます。本書での機能上のモデルでは、アセットオーナーがガバナンス、サイバーセキュリティリスクに関する判断及び運用上のエビデンスを提供します。システムインテグレーターはアーキテクチャー、設定、設置、検証及び受入れのエビデンスを提供し保守サービスプロバイダーは要員、アクセス、作業及び変更の記録を提供します。製品サプライヤーはセキュア開発、コンポーネントのセキュリティ能力、脆弱性管理及びライフサイクルに関するエビデンスを提供します。企業情報及び法域に関する情報は、これらの組織又は規制対象の設備供給・保守委託の関係に含まれる他の当事者が保有する場合があります。

したがって、届出書に記載する重要な事項ごとに、裏付け資料の管理責任者、対象範囲、該当する場合の現行版又は実施状況、及び更新の契機を明確にする必要があります。契約では、関係当事者が提供すべき情報及びエビデンス、該当する場合の直接提出に関する取り決め、秘密保持に関する要求事項及び届出済みの情報に影響し得る変更の通知を定めるべきです。内閣府の説明会資料は、導入等計画書の提出前に、直接提出が必要な書類の提出状況を確認するよう推奨しています。[5]

適合性評価又は認証の結果がセキュリティの信頼性裏付けられるのは、実際に評価された範囲に限られます。製品、コンポーネント又はサービスプロバイダーのエビデンスだけでは、システムのリスクアセスメント、セキュアなインテグレーション、運用上のエビデンス、又は経済安全保障推進法が求める法律・企業・法域に関する情報に代わるものとはなりません。

4.ギャップと実装上のリスク

残る対応範囲の差異は、残されたギャップは経済安全保障推進法に基づく制度又は ISA/IEC 62443 の不備ではなく、両者の目的と適用範囲の違いによるものです。経済安全保障推進法第 3 章の基幹インフラ制度は、法的拘束力のある経済安全保障上の審査制度であるのに対し、ISA/IEC 62443 は、産業用オートメーション及び制御システムのサイバーセキュリティに関する国際規格群です。

ISA/IEC 62443 に基づいて定められた対象範囲について作成されたエビデンスが、その範囲を超える経済安全保障推進法の要求事項への対応にも十分であるとみなされる場合、実装上のリスクが生じます。製品、システム、サービスプロバイダー又は運用に関するエビデンスは経済安全保障推進法の届出内容の裏付けとなりえますが、それだけで法令の適用可否を判断したり、必要な企業情報や法域に関する情報開示に代わったり、政府による審査・判断を代替したりすることはできません。

4.1 ISA/IEC 62443 の適用範囲外となる要求事項

経済安全保障推進法の主要な要求事項の中には、ISA/IEC 62443 に直接対応する要求事項がないものが数多くあります。ISA/IEC 62443 は、事業又は事業者が第 3 章の規制対象に含まれるか、設備が特定重要設備に該当するか、業務が重要維持管理等に該当するか、または法定届出が必要かどうかを判断するものではありません。また、事前届出手続、実施禁止期間、政府による審査手続、勧告、命令、情報提供の要請又は立入検査など事業所管大臣が所管する手続きや措置定めるものでもありません。[1,3–5,8]

ISA/IEC 62443 は、経済安全保障推進法の審査で用いられる企業情報や経済安全保障関連情報の開示についても規定していません。これには、所定の所有関係及び役員情報、議決権の直接保有者、関連する外国政府との関係、法域に伴うリスク、製造又はサービス提供場所、該当する場合の事業の安定性及び過去の法令遵守状況などが含まれます。サイバーセキュリティに関するサプライヤー管理は関連する運用リスクの管理に役立つ場合がありますが、こうした法的要求事項やデューデリジェンスに関する要求事項に代わるものではありません。

ISA/IEC 62443 に基づく技術的・組織的な変更管理プロセスは、変更がサイバーセキュリティに与える影響の評価を支援できます。しかし、その変更について経済安全保障推進法上の事前届出、事後報告、新たな計画書の提出が必要か、あるいは届出は不要かを判断するものではありません。これらの判断は、法律、適用される省令、届出要領及び所管省庁による評価に基づきます。

4.2 部分的に対応する領域

経済安全保障推進法の措置がサイバーセキュリティの保証と、より広範なサプライチェーン又は経済安全保障上の事項を組み合わせている場合、対応関係は部分的なものとなります。ISA/IEC 62443 は、サプライヤー及びサービスプロバイダーに対するセキュリティ要求事項、要員の力量、セキュアなサービス提供、開発プロセスの保証及び技術的エビデンスを支援できます。経済安全保障推進法ではこれらに加え、所有関係、役員、議決権保有者、製造又はサービス提供場所、外国政府との関係、再委託に関する取り決め及びその後の変更に関する情報が求められる場合があります。開発・製造に関する保証にも同様の境界があり、ISA/IEC 62443-4-1 はセキュアな製品開発を支援しますが、製造品質、拠点のセキュリティ又は経済安全保障全般を扱う枠組みではありません。

製品サポートの継続性も、製品の脆弱性管理やパッチ管理だけにとどまりません。ISA/IEC 62443 は、脆弱性対応、セキュリティ更新、緩和措置及びライフサイクル計画を支援できます。一方、経済安全保障推進法では、サプライヤーからのサービスが利用できなくなった場合の影響や特定社会基盤役務の安定的な提供を維持するために必要な代替手段を、指定事業者に検討を求める場合があります。したがって、こうした広範な依存関係及び継続性への対応には、調達、サプライチェーン及び運用上の追加措置が必要となります。

4.3 実装時によく見られる不備

表 12. 実装時によく見られる不備

不備の内容	想定される影響	是正措置
経済安全保障推進法の適用範囲を確認する前に、汎用的な ISA/IEC 62443 チェックリストから着手する。	法定の適用要件、規制対象設備又は分野別の届出要件と一致しない管理策やエビデンスにリソースを投入するおそれがある。	供給者選定、契約及び詳細な技術設計の前に、経済安全保障推進法の適用可否及び届出要否を判断する段階を設ける。

不備の内容	想定される影響	是正措置
機器を販売・流通させているという理由だけで製品サプライヤーの役割を割り当てる。	実際の製品開発者及び保守担当者が、セキュリティ対応とエビデンス管理のプロセスに関与しないおそれがある。	実際の開発、保守、インテグレーション及びサービス提供の責任に従って ISA/IEC 62443 上の役割を割り当てる。
コンポーネント認証をシステムセキュリティの十分なエビデンスとみなす。	そのエビデンスではオートメーションソリューション全体のリスクアセスメント、アーキテクチャー、統合、設定、受入れ及び継続運用を証明できない。	製品・コンポーネントのエビデンスに、ISA/IEC 62443-3-2 のリスク分析、ISA/IEC 62443-3-3 のシステム要求事項、統合のエビデンス及び運用記録を組み合わせる。
安全なリモートアクセスだけで保守リスクに十分対応できるとみなす。	委託先の身元、要員、作業場所、再委託、所有関係、法域及び外部からの影響が未対応となるおそれがある。	技術的なアクセス制御と併せて、経済安全保障推進法が求める企業、契約、法域及びサプライチェーンの情報を評価する。
届出の直前になって情報とエビデンスを収集する。	直接提出分の不足、供給者情報の不備又は企業記録の未更新により、届出の受理及び審査開始が遅れるおそれがある。	調達契約及びサービス契約で、情報開示義務、エビデンスに対する責任、提出期限及び更新が必要となる条件を定める。
管理策の文書化を管理策が有効に実施されていることの証明とみなす。	方針や手順は存在しても、導入、運用、試験又は是正措置の実施を示す記録がない場合がある。	各措置が文書化、実施、検証及び維持されているかを評価し、それぞれの状況を示すエビデンスを保存する。
届出後の変更を監視しない。	設備、コンポーネント、供給者、所有関係、アクセスの仕組み又は委託先の変更により、認識されないまま届出・報告義務が生じるおそれがある。	変更の受付、技術的・規制上の影響評価、エビデンスの更新及び必要な経済安全保障推進法の届出を行う継続的なプロセスを運用する。
重要維持管理等の委託契約の自動更新は経済安全保障推進法上の影響がないとみなす。	サービス範囲に変更がない場合でも、必要な委託の届出を見落とすおそれがある。	規制対象の重要維持管理等に関する契約の更新を、その都度規制上の確認の機会と位置付け、更新の効力発生前に適用される届出要件を確認する。

4.4 実装上の課題

既設設備及びレガシーシステム

長期にわたり運用されるインフラには、サポートが終了しているか、あるいは現行のセキュリティ要求事項を満たすために必要な技術的機能を備えていないハードウェアやソフトウェアが含まれる場合があります。ISA/IEC 62443-2-1 はこうした状況を想定し、機器自体に必要な機能がない場合に、アセットオーナーのセキュリティプログラムに補完的なセキュリティ対策を組み込むことを認めています。

レガシーシステムの制約があるというだけで、追加の対応を行わない理由にはなりません。アセットオーナーはこうした制約を文書化し、関連するサイバーセキュリティリスクを評価し、適切な補完的措置を特定するとともに、該当する場合にはその実施状況と有効性のエビデンスを維持すべきです。その措置を経済安全保障推進法のリスク管理措置の裏付けに用いる場合は、内閣府の説明会資料に記載された同法上の別の概念である「同等のリスク管理上の取組」と区別する必要があります。

遠隔・海外・多層的な委託関係

遠隔又は海外で業務を実施するという理由だけで、保守に関する取り決めが第 3 章の制度から外れることはありません。適用可否は、実施する業務が所定の重要維持管理等に該当するかどうかによります。識別・認証、認可、データフローの制限、システムの完全性及びイベントの記録に関する技術的管理策は、リモートアクセスに伴う IACS のサイバーセキュリティ上の課題に対応できます。一方、経済安全保障推進法では委託先、再委託先、作業場所、企業間関係及び法域に伴うリスクに関する情報が別途求められる場合があります。

特定重要設備の導入と重要維持管理等では、情報開示の考え方も異なります。特定重要設備の導入では、情報開示の対象は適用される省令が定める構成設備の供給者までであり、すべての上流供給者に自動的に及ぶわけではありません。重要維持管理等では、情報開示の対象は原則として規制対象業務を実際に行う組織まで委託関係に沿って及びます。ただし、さらに下位の再委託先については適用規則に従います。したがって、組織は、規制上の情報開示の関係とサイバーセキュリティ及び継続性の分析に用いる技術的な依存関係を区別すべきです。

直接提出とプロジェクトのスケジュール

所定の情報及び裏付け書類の一部は、関係する情報保有者から事業所管大臣に直接提出できる場合があります。これにより、商取引上の関係者を通じた機密情報の不必要な開示を減らせますが、指定事業者は引き続き届出の調整に責任を負います。提出物の一覧表を使えば、保護すべき内容を複製せずに、情報の保有者、提出状況、対象範囲及び変更状況を管理できます。

経済安全保障推進法の適用可否、エビデンスの保有責任及び直接提出に関する取り決めは、最終的な試運転・立ち上げの段階ではなく、調達・プロジェクト計画の段階で扱うべきです。法定の実施禁止期間は通常、必要な届出が受理可能となって初めて始まります。内閣府の説明会資料によれば、該当する直接提出分を含め、必要な届出資料が受領されるまで審査は開始できません。規制対象の範囲、保守委託関係又は必要な裏付けとなるエビデンスが不明確な場合は、早い段階で所管省庁に相談することが適切です。[4,5]

4.5 エビデンスの十分性

本書では、エビデンスを「文書化されている」「実施されている」「有効である」という 3 つの分析上の水準でとらえます。これらは経済安全保障推進法又は ISA/IEC 62443 の公式な分類ではありません。「文書化されている」エビデンスは、承認された方針、手順、アーキテクチャー、仕様又はその他の管理策の記述が存在することを示します。「実施されている」エビデンスは、措置が実際に導入又は実施されており、最新の記録で裏付けられることを示しています。「有効である」エビデンスは、適切な検証、監視、試験、演習又はレビューを通じ、対象設備又は保守に関する取り決めについて措置が意図したとおりに機能していることを示します。

文書があるだけでは、経済安全保障推進法の届出に十分とは限りません。内閣府の資料では、選択したリスク管理措置の実施状況を示す裏付け書類を求められています。これらの書類の形式は定められていませんが、関連する措置が実際に講じられていることを示す必要があります。

エビデンスは最新の状態を保つ必要があります。設備、製品、サプライヤー、役員、製造又はサービス提供場所、リモートアクセスに関する取り決め、再委託先又はリスク管理措置の変更は提出済み情報に影響し、事前届出、事後報告、場合によっては新たな計画書を必要とすることがあります。したがって、指定事業者は届出を一度きりの文書作成作業とせず、追跡可能な最新のエビデンスを維持すべきです。

5. 業界関係者向けガイダンス

これまでの対応付け及びギャップ分析は、IACS に関係する経済安全保障推進法に基づく届出に関与する組織にとって実務上重要な意味を持ちます。指定された特定社会基盤事業者が引き続き法定の届出主体である一方、技術的活動、企業情報及び裏付けとなるエビデンスは、関連システムを運用、統合、保守及び供給する組織に分散している場合があります。以下では、適用される経済安全保障推進法の要求事項に代わるものでないことを前提に、各組織の機能上の役割がサイバーセキュリティ及びエビデンスに関するプロセスをどう支援できるかに焦点を当てます。

5.1 アセットオーナー

アセットオーナーは、経済安全保障推進法の適用判定と整合を図りながら、規制対象設備のサイバーセキュリティの対象範囲及び要求事項を定めるべきでです。ISA/IEC 62443-3-2 は、SUC の定義、ゾーン及びコンジットの設定、サイバーセキュリティリスクの評価、SL-T の決定及びシステムセキュリティ要求事項の文書化の基礎となります。ISA/IEC 62443-3-3 は、関連するシステムレベルの技術的要求事項を規定しています。これらの活動は届出のうちサイバーセキュリティに関する事項への対応支援しますが、経済安全保障推進法の適用可否を判断したり、別途必要な企業情報及び法域に関する要求事項を満たしたりするものではありません。

調達及びサービスに関する取り決めでは、サイバーセキュリティ要求事項、裏付けとなるエビデンス、脆弱性への対応ライフサイクルを通じたサポート、再委託先の管理、直接提出並びに関連する変更の通知について責任分担を明確にすべきです。指定事業者は、必要な各情報を誰が保有しているか、それらが適切な届出経路で提出されているかを把握できるようにしておくべきです。
導入後、アセットオーナーは、設備、コンポーネント、サプライヤー、アクセスに関する取り決め、委託先、再委託先及び関連する企業・運用情報の変更を継続的に評価するプロセスを維持すべきです。技術的な変更承認と、その変更について経済安全保障推進法上の事前届出、事後報告又は新たな計画書が必要かどうかの判断は区別する必要があります。

5.2 システムインテグレーター

システムインテグレーターは、アセットオーナーのサイバーセキュリティリスクに関する判断及びシステムセキュリティ要求事項を、オートメーションソリューションのアーキテクチャー、設定及び統合に反映すべきでです。関連する活動には、ゾーン、コンジット、インターフェース及びアクセス経路の定義、セキュリティ機能と承認済みの補完的措置の実装、システムで使用する製品、バージョン、ファームウェア、ソフトウェア及び設定と要求事項とのトレーサビリティの維持が含まれます。

統合に関するエビデンスには、該当する場合、実際に構築されたシステム構成、設定の基準情報、設置時の管理策、セキュリティ検証結果、特定された逸脱事項、未解決事項及び正式な引継ぎ情報を含めるべきでです。製品の代替、アーキテクチャーの変更又は新たなアクセス経路が、システムのリスクアセスメント、受入判断の根拠又は経済安全保障推進法に基づく提出済み情報に影響し得る場合は、実施前に連絡すべきです。

5.3 保守サービスプロバイダー

保守サービスプロバイダーは、アクセスする設備、実施する業務、関係要員、作業場所、リモートアクセスの方法及び再委託先を含め、実際のサービス範囲を定めるべきでです。ベンダー、マネージドサービスプロバイダー又はエンジニアリング請負業者などの商取引上の呼称によって、業務が重要維持管理等に該当するかどうかは決まりません。

ISA/IEC 62443-2-4 は、インテグレーション及び保守サービスにおける管理されたプロセスについて主要な要求事項を定めています。保守サービスプロバイダーは、明確な責任分担、要員の力量、承認済みの手順、アクセスの認可、変更管理、作業記録及びインシデント発生時のエスカレーション体制を維持すべきです。遠隔保守は管理された特権アクセスとして扱い、適切な認可と監視を行うべきでです。記録には、関係する申請者又は承認者、対象システム、目的、アクセス期間、担当者及び実施した作業を明記すべきです。適用される経済安全保障推進法の届出要領で求められる場合は、実際の遠隔作業場所及び関連する再委託の取り決めについても明らかにする必要があります。

アセットオーナーからパッチ関連業務を委任されている場合、保守サービスプロバイダーは、該当するサプライヤー情報、影響評価、承認、パッチの適用及びロールバックの記録を調整すべきです。再委託は規制対象業務に応じて管理し、適用される経済安全保障推進法のリスク管理措置で求められる場合は、指定事業者の承認及び再委託先による同等のサイバーセキュリティ対策を含めるべきです。関係要員、アクセスに関する取り決め、作業場所又は再委託先の変更が届出内容又はサイバーセキュリティ上の判断根拠に影響し得る場合は、その変更を連絡すべきです。

5.4 製品サプライヤー

本書の対象範囲では、製品サプライヤーは、セキュリティ要求事項、セキュアなな設計と実装、検証及び妥当性確認、欠陥管理、パッチ管理並びに製品のライフサイクル終了を含む、セキュアな製品開発ライフサイクルを維持すべきです。また、アセットオーナー及びシステムインテグレーターがシステムのリスクアセスメントと統合を行うために必要な、セキュリティ機能、設定に関するガイダンス、使用環境の前提条件、既知の制約及び脆弱性対応に関する情報を提供すべきでです。

製品セキュリティに関するエビデンスには、サポート期間、脆弱性報告手順、セキュリティ更新に関する取り決め、サポート終了条件及び利用可能な移行・代替手段に関するライフサイクル情報を添えるべきです。これらの記録はサイバーセキュリティ及び継続性の分析を支援しますが、システムレベルの統合又は運用に関するエビデンスにに代わるものではありません。

製品サプライヤーが経済安全保障推進法の関連する情報提供の対象範囲に含まれる場合、所定の企業情報、製造場所、コンポーネントサプライヤー又は法域に関する情報を別途提供する必要が生じることがあります。契約では、提出済み情報又は継続的な製品サポートに影響し得る変更の通知を定めるべきです。所定の情報又は裏付け資料を直接提出できる場合、サプライヤーは適用される届出手続に従って提出を完了し、指定事業者に提出状況について適切な確認情報を提供すべきです。

5.5 関係者間の連携

4 つの機能上の役割は、経済安全保障推進法の適用判定と役割分担から始まり、サイバーセキュリティのリスクアセスメントと要求事項、デューデリジェンスと契約、届出・エビデンスの準備、届出と審査、実装と受入れ、継続的な運用と変更レビューへと進む、共通のライフサイクルの中で連携させるべきです。これらの作業は並行して進められる場合もありますが、法定の届出を、試運転・立上げの最終段階でのみ行う作業として扱うべきではありません。

役割	1. 適用判定と役割の割当て	2. リスク評価とセキュリティ要求事項	3. デューデリジェンスと契約
特定社会基盤事業者（法定届出主体） ESPA上の法的責任	ESPAの適用範囲と届出義務を確認	規制上の要求事項と分野別基準に整合させる	契約に基づく情報及び証拠資料の提供を調整
アセットオーナー（運用者） 機能上最も近い位置付け	運用範囲と規制対象設備を定義し、機能上の役割を割り当てる	システムリスクアセスメントを行い、SL-Tとシステムセキュリティ要求事項を定義	デューデリジェンスを主導し、開示義務と必要な証拠資料を定める
システムインテグレーター（IACSサービスプロバイダー） ソリューションの設計・実装	対象範囲とインターフェースを把握し、技術的境界を確認	アーキテクチャ、ゾーン、コンジットを定義し、システム要求事項を満たしSL-Tを支援する機能を選定・統合	技術情報を提供し、証拠資料の提出を約束
保守サービスプロバイダー 保守及びサポートの提供	サービス範囲（設備、機能、場所、要員、再委託先）を定義	保守リスクを評価し、アクセス及び運用上の要求事項を定義	委託先情報を提供し、保守・セキュリティ体制を確認
製品サプライヤー（開発者・保守者） 製品の開発・保守	製品の役割（開発者・保守者）と対象範囲を確認	製品セキュリティ要求事項及びライフサイクル支援を定義	製品情報、セキュリティ機能及び脆弱性対応支援を提供

役割	4. 届出及び証拠資料の準備	5. 届出と審査	6. 実装と受入れ	7. 運用と変更レビュー
特定社会基盤事業者（法定届出主体） ESPA上の法的責任	届出資料一式及び直接提出を調整	計画書及び所定情報を提出し、所管省庁と連絡	実施禁止期間の満了・短縮を確認し、開始前に勧告・命令に対応	変更を監視し、報告又は新規計画書の提出義務に対応
アセットオーナー（運用者） 機能上最も近い位置付け	リスク管理措置を承認し、証拠資料の十分性を確認	求めに応じて審査に協力	システム又はサービスを受け入れ、運用準備の整備状況を承認	運用、変更及び継続的なリスクレビューを管理
システムインテグレーター（IACSサービスプロバイダー） ソリューションの設計・実装	システム構成、設定、統合及び試験結果を証拠資料として準備	求めに応じて説明及び証拠資料を提供	据付検証及び受入試験を支援	変更、更新及び証拠資料の維持を支援
保守サービスプロバイダー 保守及びサポートの提供	アクセス管理、保守プロセス及び要員能力に関する運用証拠を準備	審査に関する照会への回答を調整	保守サービスを提供し、記録と監視を維持	変更、再委託先及び報告が必要となる事由を監視
製品サプライヤー（開発者・保守者） 製品の開発・保守	安全な開発ライフサイクルの記録、SL-C（コンポーネント）、既知の制約及びサポート情報を提供	求めに応じて追加情報を提供	脆弱性対応及び更新を支援	届出済み情報又はサポートの提供可能性に影響する変更を通知

役割間の継続的な調整 **継続的な監視と変更管理**

ESPAの届出・審査

必要な資料（直接提出分を含む）がすべて受領されて初めて、届出の受理及び審査の開始が可能となる。

図 4. 役割別の経済安全保障推進法対応準備及び保証ライフサイクル

製品、システム、運用及び法規制に関するエビデンスは、対象範囲と保有責任を区別しながら、共通の保証プロセスの下を通じて連携されるべきです。重要な届出項目又は裏付けとなるエビデンス一式ごとに、該当する場合、保有責任者、現状及び更新の契機を明確にすべきです。契約では、エビデンス及び情報の提供、直接提出の調整、秘密保持に関する取り決め及び関連する変更の通知を定めるべきです。ISA/IEC 62443 はこのプロセスのサイバーセキュリティに関する部分を強化できますが、適用される法的要求事項、企業情報及び法域に関する要求事項又は政府審査に関する要求事項に代わるものではありません。

6. 結論

経済安全保障推進法と ISA/IEC 62443 は、それぞれ異なる責任を扱いますが、相互に補完する関係にあります。第 3 章は、特定重要設備の導入及びその重要維持管理等の委託について事前届出と政府審査の法的枠組みを定めています。ISA/IEC 62443 は、IACS のサイバーセキュリティを管理するための組織、システム、サービスプロバイダー及び製品に関する要求事項とプロセスを規定しています。

最も強い対応関係が見られるのは、サイバーセキュリティガバナンス、システムのリスクアセスメント、セキュリティ要求事項、管理された統合と保守、セキュアなな製品開発、脆弱性管理、インシデント対応及び復旧です。経済安全保障推進法はこうした領域以外にも、企業の所有・支配関係、法域に伴うリスク、外国政府との関係、製造・サービス提供場所、サプライヤーへの依存、法定の情報開示及び政府審査を対象としています。したがって、ISA/IEC 62443 に基づくエビデンスは、経済安全保障推進法全体への適合を証明するものではありませんが、同法に基づく届出のうちサイバーセキュリティに関する事項を裏付けることができます。

実務上、指定事業者は規制対象範囲を定め、各関係者が実際に担う機能に従って責任を割り当て、最新の裏付けとなるエビデンスを入手し、関連する変更を評価するプロセスを維持する必要があります。製品、システム、運用及び法規制に関するエビデンスは、それぞれの対象範囲と保有責任者を追跡できる状態に維持すべきです。このように活用することで、ISA/IEC 62443 はサイバーセキュリティの保証に体系的な基礎を提供すると一方、適用される経済安全保障推進法の法的要求事項、情報開示及び審査に関する要求事項に別途対応する必要があります。

用語集

用語	本書における意味
達成セキュリティレベル（SL-A）	実装されたオートメーションソリューションの対象となるゾーン又はコンジットで、実際に達成したセキュリティレベル。ISA/IEC 62443-4-2 に基づくコンポーネントのセキュリティ能力に関する主張によって確立されるものではない。
アセットオーナー	IACS を所有又は運用し、そのサイバーセキュリティプログラム、リスク判断及びシステムセキュリティ要求事項に責任を負う組織。指定事業者との機能上の対応関係が最も近いものとして用い、法的な同義語としては用いない。
オートメーションソリューション	IACS に必要な制御、安全及び補完的な機能を実現する技術的ソリューション。IACS 内で動作するように設置・設定されたハードウェア及びソフトウェアのコンポーネントからなる。
事業所管大臣	指定、届出、審査及び関連する規制上の措置を含め、対象分野の第 3 章の施行を所管する大臣。
コンポーネントの能力セキュリティレベル（SL-C（コンポーネント））	ISA/IEC 62443-4-2 に基づく IACS コンポーネントの能力セキュリティレベル。オートメーションソリューション全体の SL-T 又は SL-A を確立するものではない。
委託先	経済安全保障推進法の適用範囲内で重要維持管理等を実施するため、特定社会基盤事業者から直接委託を受ける個人又は組織。経済安全保障推進法上の委託関係での位置付けを表し、それ自体で ISA/IEC 62443 上の保守サービスプロバイダーの役割が定まるわけではない。
制御システムの能力セキュリティレベル（SL-C（制御システム））	ISA/IEC 62443-3-3 が定める制御システムの技術的要求事項に対応する能力セキュリティレベル。SL-T 及び SL-A とは異なる。
重要維持管理等	適用される分野別省令で「重要維持管理等」として定められた業務を指す、本書で用いる簡略表現。
指定事業者	本書で特定社会基盤事業者を指す略称。
直接提出	関係する供給者、委託先、再委託先又はその他の情報保有者が、指定事業者を経由せず、所定の情報又は裏付け書類を事業所管大臣に直接提出することが認められる場合に用いる、本書での実務上の用語。
経済安全保障推進法	日本の「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和 4 年法律第 43 号、改正を含む）。
IACS	産業用オートメーション及び制御システム。ISA/IEC 62443 のモデルでは、IACS はオートメーションソリューションと、その設計、導入、運用及び保守に必要な組織的措置からなる。
保守サービスプロバイダー	オートメーションソリューションの保守又は運用支援を行う機能上の役割。実際の業務が規制対象の重要維持管理等に該当する場合に限り、経済安全保障推進法上の委託先又は再委託先に対応する。

用語	本書における意味
省令で定める構成設備	適用される省令で定められ、関連する届出要件に基づいて供給者その他の情報の提出が必要となる構成設備を指す、本書での実務上の用語。
製品サプライヤー	ISA/IEC 62443-4-1 において、対象となる IACS 製品の開発又は保守に責任を負う組織。機器の販売、流通、組立又は設定を行うだけで、この役割が該当するわけではない。
特定重要設備	第 3 章の適用上、該当する分野別省令で定められる施設、装置、機器又はプログラム。
特定妨害行為	特定妨害行為の英訳として現行の内閣府の英語資料では、「specified disruptive action」が、一部の参考英訳では「specified interference action」を用いられている。
特定社会基盤事業者	第 3 章に基づき事業所管大臣から正式に指定された事業者。対象となる導入等計画書の法定の届出主体となる。
再委託先	重要維持管理等の委託関係において、委託先又は他の再委託先から関連業務を委託される個人又は組織。届出に関係するかどうかは適用される省令及び実際に行う業務による。この用語だけで ISA/IEC 62443 上の役割が定まるわけではない。
特定重要設備の供給者	特定重要設備としての機能を果たせる状態で、その設備を製造又は供給する者。特定社会基盤事業者に単に設備を販売する者は含まれず、供給者が必ずしも事業者の直接の契約相手とは限らない。この用語は経済安全保障推進法上の供給関係での位置付けを表し、それだけで ISA/IEC 62443 上の役割が定まるわけではない。
構成設備の供給者	適用される省令で定められた構成設備を、その機能を果たせる状態で製造又は供給する者。特定重要設備の供給者に構成設備を単に販売する者は含まれない。すべての上流の部品供給者を指すわけではなく、この用語だけで ISA/IEC 62443 上の製品サプライヤーの役割が定まるわけでもない。
システムインテグレーター	オートメーションソリューションの設計、設定、統合、設置、試験又は試運転を行う機能上の役割。経済安全保障推進法では独立した法定の役割名として用いない。
検討対象システム（SUC）	ISA/IEC 62443-3-2 のサイバーセキュリティリスクアセスメントのために定義するシステムの境界。
目標セキュリティレベル（SL-T）	ISA/IEC 62443-3-2 のリスクアセスメントを通じ、対象となる各ゾーン及びコンジットに対して設定される目標セキュリティレベル。

参考文献

日本語の法律、政令、省令及び公式告示が優先する。英訳及び内閣府の英語資料は参照用であり、最新の日本語原文と適用される施行規定を確認する必要がある。オンライン資料の最終確認日は 2026 年 8 月 14 日である。

[1] 日本政府：

(a)「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和 4 年法律第 43 号）。令和 8 年法律第 38 号による改正を含み、適用される施行規定に従う。e-Gov 法令検索。

(b)「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律施行令」（令和 4 年政令第 394 号、改正を含む）。e-Gov 法令検索。

[2] 内閣、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本的な方針」、2022 年 9 月 30 日閣議決定。

[3] 内閣、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」、2023 年 4 月 28 日閣議決定。

[4] 内閣府、「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」（詳細版）、2026 年 7 月 7 日版。

[5] 内閣府、「経済安全保障推進法における特定社会基盤役務の安定的な提供の確保に関する制度（説明会資料）」、2026 年 7 月 7 日版。

[6] 内閣府、「特定社会基盤事業者として指定された者」、2026 年 7 月 1 日現在。

[7] 日本政府、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律及び株式会社国際協力銀行法の一部を改正する法律」（令和 8 年法律第 38 号、2026 年 6 月 17 日公布）。併せて内閣府「経済安全保障推進法及び株式会社国際協力銀行法の一部を改正する法律案の概要」（2026 年）を参照。

[8] 内閣府、「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」、2026 年 3 月 31 日版。

[9] 法務省、日本法令外国語訳データベース、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（参考英訳）。英訳に法的権威はなく、現行の日本語の法律及び 2026 年改正と照合する必要がある。

[10] ISA, ISA/IEC 62443 Series of Standards（規格群の概要、関係者の役割及び責任分担についての説明）。

[11] IEC, Industrial communication networks: Network and system security, Part 1-1: Terminology, concepts and models, IEC TS 62443-1-1:2009, Geneva, Switzerland, 2009.

[12] IEC, Security for industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners, IEC 62443-2-1:2024, Geneva, Switzerland, 2024.

[13] IEC, Security for industrial automation and control systems, Part 2-2: IACS security protection scheme, IEC PAS 62443-2-2:2025, Geneva, Switzerland, 2025.

[14] IEC, Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment, IEC TR 62443-2-3:2015, Geneva, Switzerland, 2015.

[15] IEC, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers, IEC 62443-2-4:2023, Geneva, Switzerland, 2023.

[16] IEC, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design, IEC 62443-3-2:2020, Geneva, Switzerland, 2020.

[17] IEC, Industrial communication networks: Network and system security, Part 3-3: System security requirements and security levels, IEC 62443-3-3:2013, Geneva, Switzerland, 2013. The current IEC copy incorporates Corrigendum 1:2014.

[18] IEC, Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1:2018, Geneva, Switzerland, 2018.

[19] IEC, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, IEC 62443-4-2:2019, Geneva, Switzerland, 2019. The current IEC copy incorporates Corrigendum 1:2022.

[20] IEC, Security for industrial automation and control systems, Part 6-1: Security evaluation methodology for IEC 62443-2-4, IEC TS 62443-6-1:2024, Geneva, Switzerland, 2024.

[21] IEC, Security for industrial automation and control systems, Part 6-2: Security evaluation methodology for IEC 62443-4-2, IEC TS 62443-6-2:2025, Geneva, Switzerland, 2025. The document does not define a complete certification scheme or certification program.

[22] IEC, Security for industrial automation and control systems, Part 1-6: Application of the 62443 series to the Industrial Internet of Things (IIoT), IEC PAS 62443-1-6:2025, Geneva, Switzerland, 2025.

[23] 内閣府：

(a) 内閣府, “Outline of the Essential Infrastructure System and Required Information (As of June 2026): Introduction of Specified Critical Facilities,” 2026 年 6 月。

(b) 内閣府, “Outline of the Essential Infrastructure System and Required Information (As of June 2026): Entrustment of Critical Maintenance and Management, etc.,” 2026 年 6 月。