経済産業省

電力制御システムに関する
サプライチェーン・セキュリティ対策の手引き

2025年6月3日

産業サイバーセキュリティ研究会　ワーキンググループ1（制度・技術・標準化）
電力サブワーキンググループ（電力SWG）

1. 背景と目的

1.1. 背景・目的

電力分野に限らず、重要インフラ全体でサプライチェーンに起因するリスクが高まりつつある。

サプライチェーンが影響を受け得る代表的なリスクとしては、自然災害やパンデミックに代表される環境的リスク、テロや政治的な不安などの地政学的リスク、経済危機や原料の価格変動といった経済的リスク、サイバー攻撃やシステム障害などの技術的リスクといった、様々なリスクがある。

令和5年度に策定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」では、重要インフラ分野に共通して求められる取組として、サプライチェーンに起因するサイバーセキュリティ上のリスク（以降、本手引きにおいて「サプライチェーン・リスク」と呼ぶ）※1への対応が明記された。

関連して、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」では、安全基準等策定指針で示されたセキュリティ確保に向けた取組についての参考情報が明記されたほか、経済安全保障推進法に基づくサプライチェーン・リスクに対する取組も進んでいる。

電力分野における取組として、電力分野のサイバーセキュリティ対策について議論する電力サブワーキンググループ（電力SWG）は、電力制御システム等のサプライチェーン・リスクに対するサイバーセキュリティ上の対策（以降、本手引きにおいて「サプライチェーン・セキュリティ対策」と呼ぶ）に関する議論結果を取りまとめ、「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」を令和5年度に発表した。

この提言では、電力制御システムに関して、対応すべき代表的なサプライチェーン・リスクに対し、電気事業者において求められる取組が整理されている。また、事業者における効果的かつ実効性のある取組の実施に向け、「電力制御システムセキュリティガイドライン」の見直しを含め、関係者に求められる取組を提言しているほか、実効性ある対応に資する手引き文書の策定を提言している。

本文書は、上記の提言を踏まえ、電気事業者に求められるサプライチェーン・セキュリティ対策※2の取組を支援するために、対策の実施に関する手引きや対策の実施に当たって参考となるグッドプラクティスを示すものである。

※1: 次頁に示すとおり、本文書では、電気事業者へ電力制御システムが納入されるまでの開発や製造に関する一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスクを電力制御システムの「サプライチェーン・リスク」と定義している。本文書はサイバーセキュリティ上のリスクのみを扱い、エネルギーサプライチェーンにおけるリスク（例：自然災害に伴うエネルギーの供給途絶（環境的リスク）、国際情勢の変動に伴う燃料の調達遅延（地政学的リスク））等はスコープ外であることに留意。

(参考文書)
経済産業省, 通商白書2022 https://www.meti.go.jp/report/tsuhaku2022/index.html
NISC, 重要インフラのサイバーセキュリティに係る安全基準等策定指針 https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf
NISC, 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書 https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf
電力SWG, 電力制御システムのサプライチェーン・セキュリティ向上策に関する提言 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf

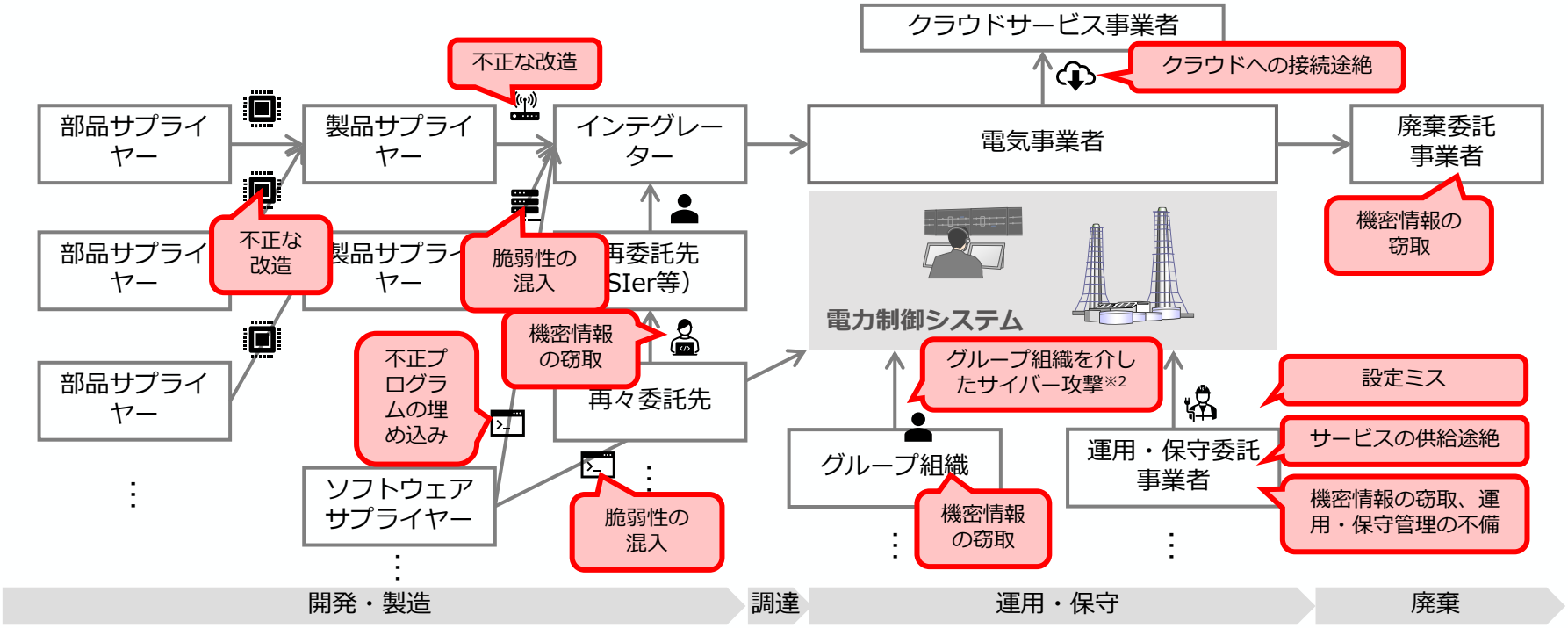
1.2. 本文書におけるサプライチェーン・リスク

本文書における電力制御システムの「サプライチェーン・リスク」とは、**電気事業者へ電力制御システムが納入されるまでの開発や製造に関する一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスク**を意味する。

電力制御システムに想定されるサプライチェーン・リスクは以下のとおりであり、開発・製造段階の不正プログラムの埋め込み、開発・製造段階や運用・保守段階での脆弱性の混入、不正操作、設定ミス等を含む※1。

これらのリスクが顕在化した場合、電力の安定供給や電気事業者の事業継続に影響を及ぼすおそれがある。

電力制御システムに想定されるサプライチェーン・リスクの例



※1: 本文書では、サプライチェーンにおけるサイバーセキュリティ上のリスクのみを扱い、エネルギーサプライチェーンにおけるリスク（例：国際情勢の変動に伴う燃料の調達遅延、自然災害に伴うエネルギーの供給途絶）等はスコープ外であることに留意。

※2: 脆弱な関連企業・グループ企業を介して本来のターゲット企業に侵入するサイバー攻撃は「アイランドホッピング攻撃」とも呼ばれ、サプライチェーン・リスクとは異なる文脈で議論されることもあることに留意。

出所）NISC、外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書等に基づき作成　https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf

1.3. サプライチェーン・セキュリティ対策の重要性

電力分野に限らず、**サプライチェーン・リスクに関する事例が発生している。**

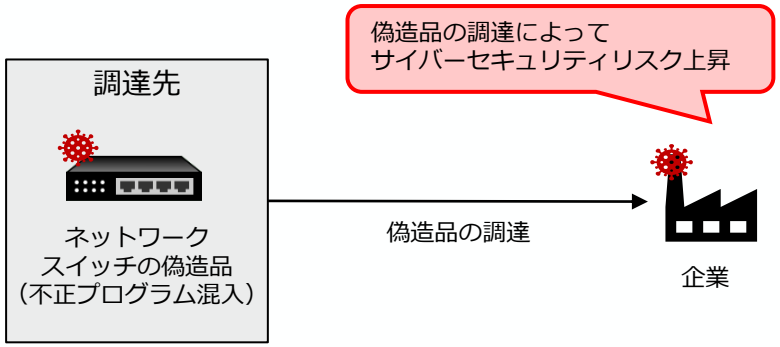
重要インフラ事業者である電気事業者においては、電力安定供給のために適切なサプライチェーン・セキュリティ対策を講じる必要があるところ、**経営層は、サプライチェーン・リスクに対処するために適切なリソース配分と体制の整備を行う必要がある。**

本文書に記載の手引きや対策のプラクティスを参照し、自組織に求められる対策の事項を整理することで、適切なリソース配分と体制の整備を行うことができる。

サプライチェーン・リスクに関する事例

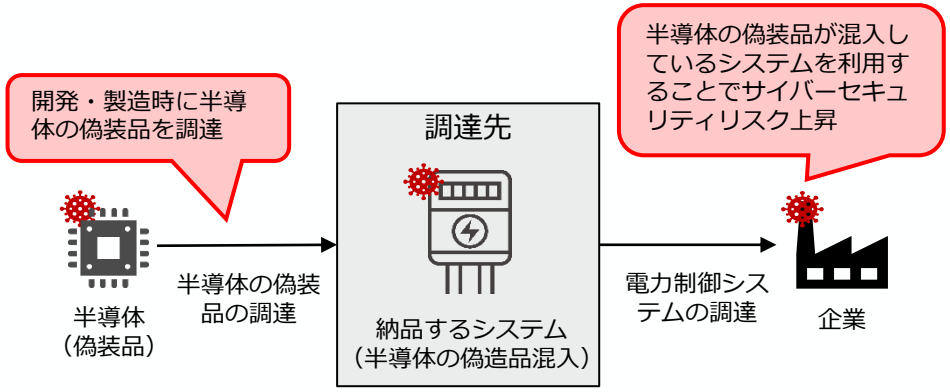
(1) ネットワークスイッチの偽造品の流通

- 2019年4月、Cisco社は同社製品の約60万ドル相当の偽造品を押収した。
- セキュリティ関連企業のF-Secure社がCisco製ネットワークスイッチの偽造品を分析したところ、ソフトウェアによる認証を回避する不正プログラムが埋め込まれていることが判明した。
- F-Secure社は、偽造品を利用した場合、サイバーセキュリティ上のリスクを高めることに繋がる可能性があると指摘した。



(2) 半導体の偽造品の流通

- 偽造品・偽装品に関するデータベースを提供するERAI社は、2023年内に、786個の半導体の偽装品及び不適合品の流通を確認し、過去2年間で件数が増加していると報告した。
- 2023年内において、正規のメーカーによって製造されている半導体の偽装品及び不適合品の流通が、全体の13.2%を占めているとのことであった。
- 半導体の偽装品にはマルウェアが搭載されるリスクがあることを、欧州刑事警察機構（Europol）が指摘している。

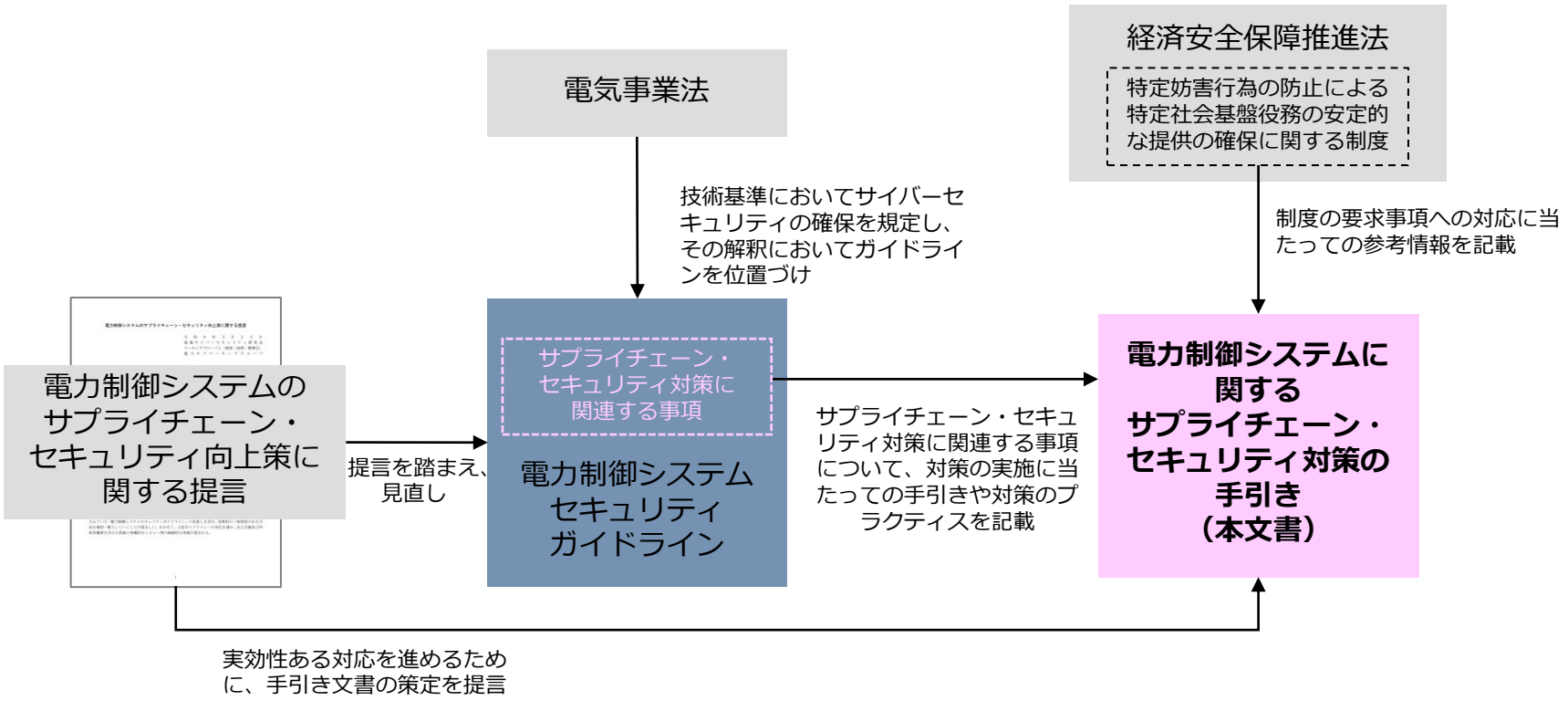


F-Secure, THE FAKE CISCO https://labs.withsecure.com/content/dam/labs/docs/2020-07-the-fake-cisco.pdf
ERAI, 2023 Annual Report https://www.erai.com/erai_blog/3183/_2023_annual_report
EUROPOL, Intellectual Property Crime Threat Assessment 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf

1.4. 本文書の位置づけ

本文書は、**「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」に記載されたサプライチェーン・セキュリティ対策に関連する事項について、事業者における対策の実施を支援・促進するために、対策の実施に当たっての手引きや対策のプラクティスを示したもの**であり、**新たな要求事項を示したものではない**。

また、経済安全保障推進法の「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制度」の要求事項への対応に向けた参考情報も示している。



(参考文書)
日本電気協会, 電力制御システムセキュリティガイドライン https://store.denki.or.jp/products/detail/702
電力SWG, 電力制御システムのサプライチェーン・セキュリティ向上策に関する提言 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf
内閣府,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 https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin2.pdf

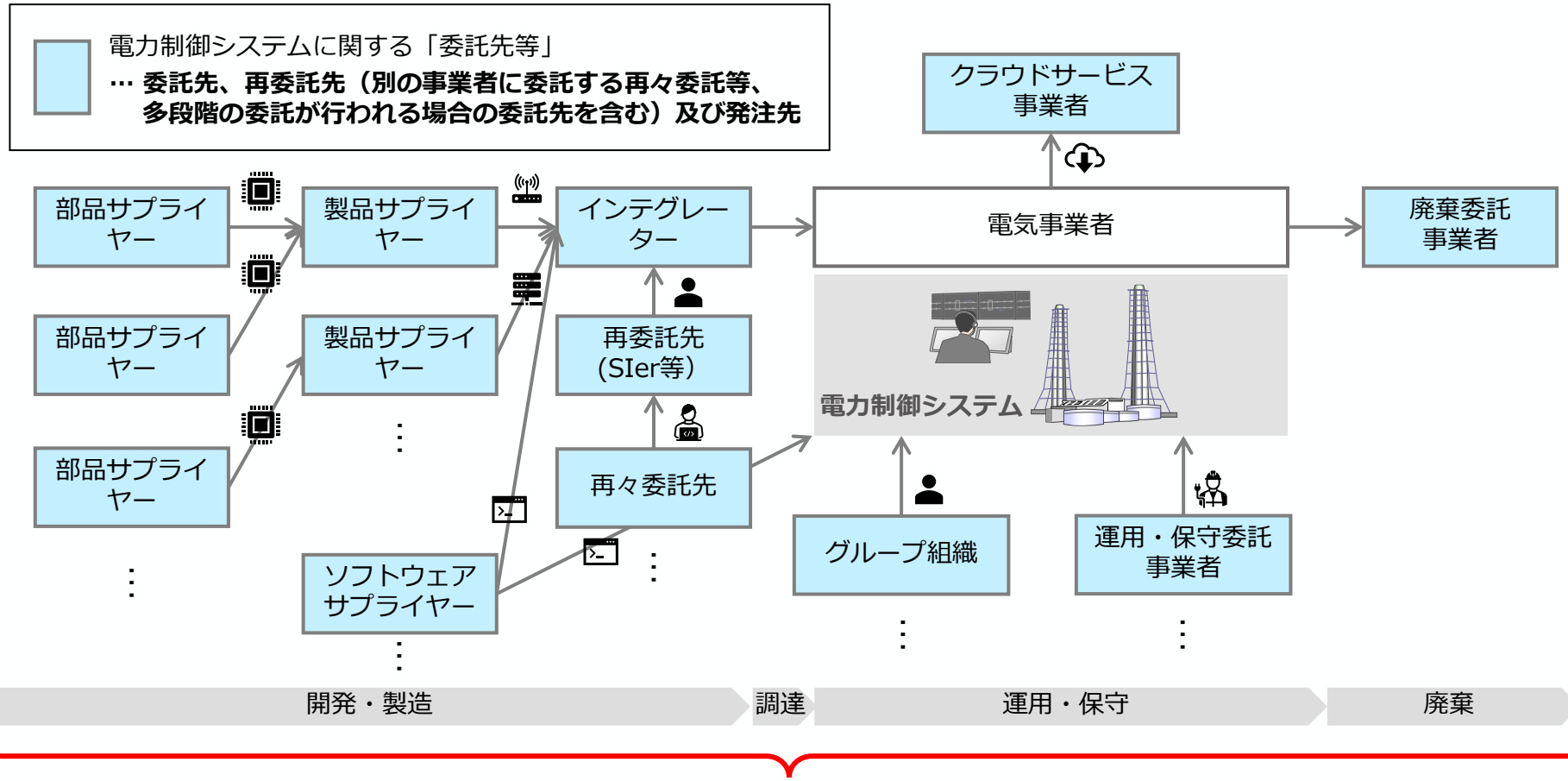
1.5. 主な対象読者・活用方法

本文書は、**電力制御システムを運用する電気事業者**のほか、**電力制御システムに関する「委託先等」**を主な対象とする。
当該事業者のうち、特に以下の部門及び関係者での活用が期待される。

	経営層、セキュリティ管理責任者	サプライチェーン関連部門（調達管理部門等）	セキュリティ関連部門
サプライチェーン・リスクに関して求められる役割	● サプライチェーン・リスク管理に関する責任 ● サプライチェーン・リスク管理方針の策定・承認 ● サプライチェーン・リスク管理体制の構築、リソースの確保 ● サプライチェーン・セキュリティ対策に対する意識醸成 ● 継続的な確認・改善	● サプライチェーンの管理 ● サプライチェーン・リスク管理計画の策定 ● サプライチェーン・セキュリティ対策に関する要求事項の検討・策定 ● 委託先等の選定・評価 ● 委託先等の管理、委託先等との連携 ● 委託先等のセキュリティ対策状況の把握	● サプライチェーン・リスク評価 ● サプライチェーン・セキュリティ対策に関する要求事項の検討・策定 ● セキュリティ対策の実装 ● 脆弱性管理、変更管理 ● インシデント発生時の対応 ● サプライチェーン・セキュリティ対策に関する教育 ● セキュリティ対策の評価・改善
期待される本文書の活用方法	● 電力制御システムに求められるサプライチェーン・セキュリティ対策の理解のために活用する。 ● 管理方針の策定に向けた指針として活用する。 ● リソース配分の際の参考資料として活用する。 ● 従業員及び委託先等への教育・啓発の際に活用する。 ● 定期的なリスク評価及び改善の指針として活用する。	● 電力制御システムに求められるサプライチェーン・セキュリティ対策の理解のために活用する。 ● サプライチェーン・リスク管理計画の策定のために活用する。 ● サプライチェーン・セキュリティ対策の検討・策定のために活用する。 ● サプライチェーン・セキュリティ対策を考慮した委託先等の選定・評価のために活用する。 ● 委託先等の管理・把握や委託先等との連携時に活用する。	● 電力制御システムに求められるサプライチェーン・セキュリティ対策の理解のために活用する。 ● サプライチェーン・リスクの評価のために活用する。 ● サプライチェーン・セキュリティ対策の検討・策定・実装のために活用する。 ● 脆弱性管理や変更管理のために活用する。 ● 従業員及び委託先等への教育・啓発の際に活用する。

1.6. 本文書における「委託先等」の範囲

本文書における「委託先等」とは、**電力制御システムに関する委託先、再委託先（別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む）及び発注先**を指す。



本文書の対象読者：
委託先・発注先を含む、電力制御システムのサプライチェーンに関係する全事業者

1. 背景と目的

2. 求められるサプライチェーン・セキュリティ対策

2.1. 求められるサプライチェーン・セキュリティ対策

2.2. 想定される対応プロセス

3. 対策の手引き・プラクティス

4. 付録

2.1. 求められるサプライチェーン・セキュリティ対策

実際にサプライチェーン・リスクが顕在化した事例も複数存在するため、電気事業者においては、想定されるサプライチェーン・リスクに対して適切な対策を講じることが求められる。

特に、「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」では、サプライチェーン・リスクに対抗するために以下の対策を実施することが提言されている。

項目	求められるサプライチェーン・セキュリティ対策	対応する「電力制御システムセキュリティガイドライン」の条項	対応するサプライチェーン・リスク
1. サプライチェーン・リスク管理	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。	第2-2条 役割	全リスク
	C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。	第4-1条 セキュリティ管理	
2. セキュリティ仕様の確認	A) 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 B) 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 C) 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。	第6-1条 セキュリティ仕様の確認	• 開発・製造時の不正な改造 • 開発・製造時の不正プログラムの埋め込み • 運用・保守時のソフトウェアの不正な更新
3. 機器の適切な管理	A) 機器の管理に関して、機器をライフサイクルを通じて管理し、保護する。	第6-2条 機器・外部記憶媒体及びデータの管理	• 調達時の不正な改造 • 調達時の不正プログラムの埋め込み • 廃棄時の機密情報の窃取

(参考文書)
電力SWG, 電力制御システムのサプライチェーン・セキュリティ向上策に関する提言 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf

2.2. 想定される対応プロセス

サプライチェーン・セキュリティ対策に関する各取組について、想定される対応のフローは以下のとおりである。

本文書では、各プロセスにおける具体的な対策の手引きや対策に関するグッドプラクティスを提供する。

1. 背景と目的

2. 求められるサプライチェーン・セキュリティ対策

3. 対策の手引き・プラクティス

3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

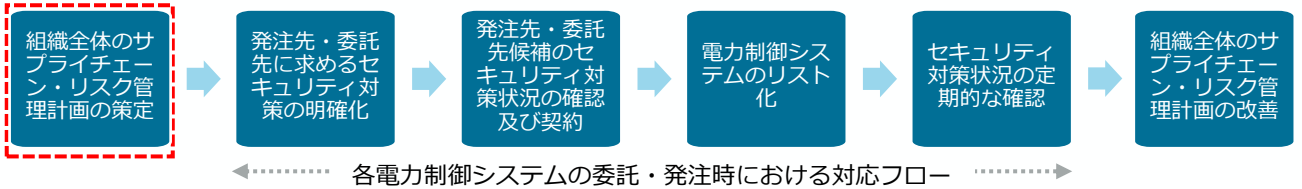
3.2. 「2. セキュリティ仕様の確認」に関する対策の手引き・プラクティス

3.3. 「3. 機器の適切な管理」に関する対策の手引き・プラクティス

4. 付録

3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。



対策実施に関する手引き

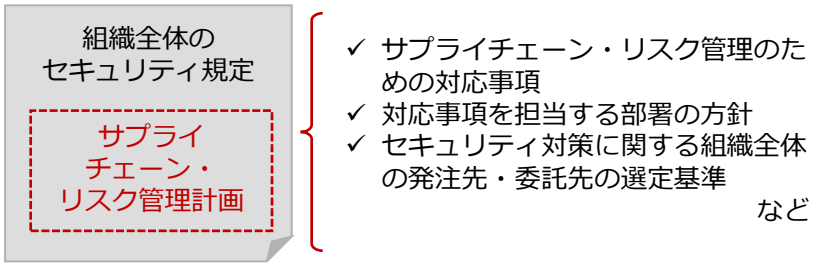
- まず、電力制御システム等のサプライチェーン・リスクを管理するための自組織内の計画を策定する。サプライチェーン・リスクに限定されないリスク管理計画がすでに存在する場合、当該計画に含める形で策定することが効果的である。サプライチェーン・リスク管理計画には以下の事項を含めることが想定される。
  - ✓ サプライチェーン・リスク管理のための対応事項
  - ✓ 対応事項を担当する部署の方針
  - ✓ セキュリティ対策に関する組織全体の発注先・委託先の選定基準

- 「セキュリティ対策に関する組織全体の発注先・委託先の選定基準」として設けるべき選定基準の例としては、以下が挙げられる。
  - ✓ 組織の管理方針に基づき、セキュリティ対策に関する管理体制を構築及び文書化し、定期的に改善していること
  - ✓ インシデント発生時の連絡体制を構築していること
  - ✓ 業務の再委託を制限すること
  - ✓ 従業員に対して、セキュリティ対策に関する教育や研修を定期的に実施していること

- 策定したサプライチェーン・リスク管理計画について、自組織の経営方針やセキュリティ方針に合致していることを確認し、経営層や関係部署の同意を得る。このために、サプライチェーン・リスク管理計画を実施する目的や目標を明確にし、サプライチェーン・リスクに対処することの重要性を経営層や関係部署に理解させる。

対策のグッドプラクティス

- 組織全体のセキュリティ規定の一部に電力制御システムのサプライチェーン・リスク管理計画を含めることで、組織全体のセキュリティの取組に整合したサプライチェーン・リスク管理計画を策定する。

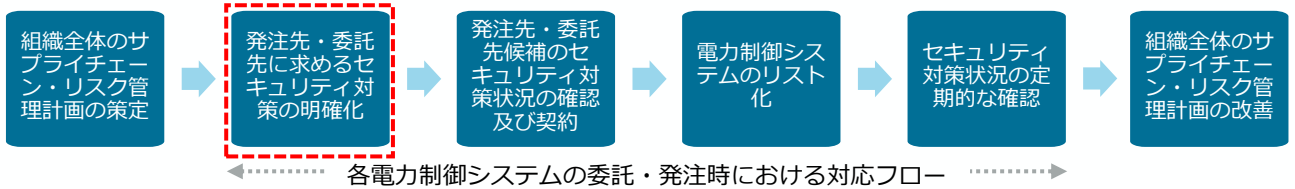


- 自組織のサプライチェーンを洗い出したうえで、事業影響度の大きいサプライチェーンを把握する。そして、当該サプライチェーンに存在するサプライチェーン・リスクを特定し、そのリスクが顕在化した場合の影響度を評価・分析したうえで、サプライチェーン・リスク管理のための対応事項を整備する。評価・分析対象とするサプライチェーン・リスクとしては、不正プログラムの埋め込みや脆弱性の混入等のリスクだけでなく、設定ミス等のリスクも考慮する。

- 自組織の電力制御システム等に関する調達・委託のプロセスを整理したうえで、サプライチェーン・リスク管理のための対応事項を担当する部署の方針を策定する。

3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。

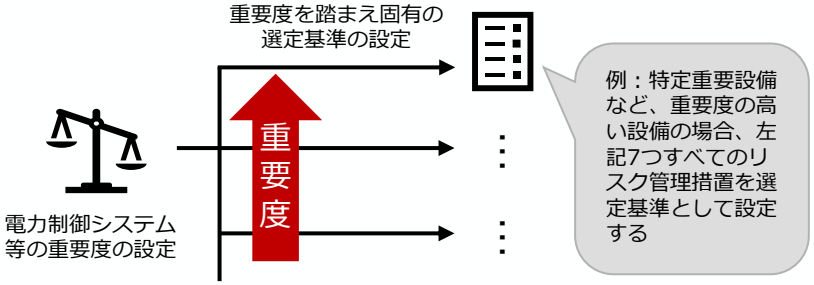


対策実施に関する手引き

- 電力制御システム等の発注や運用・保守の業務委託を実施する際には、組織全体の選定基準に加え、当該契約固有の選定基準を設けることが想定される。選定基準の例としては以下が挙げられる。
  - ✓ 意図しない変更が行われないような管理体制を整備していること
  - ✓ 不正な変更やそのおそれが確認された場合に、追跡調査や立入検査等に協力すること
  - ✓ サービス保証を行うための方法を整備していること
  - ✓ 電力制御システムを構成する重要部品の調達について、自組織と同様な選定基準で選定を行っていること
  - ✓ 外国の法的環境や外部主体の指示によって契約に違反する行為が生じた可能性がある場合、これを報告すること
  - ✓ 役員や資本関係等、事業計画や実績、設備又は部品を製造する工場等の所在地、作業に従事する者の所属・専門性に関する情報を提供すること
  - ✓ 過去3年間において、国内の法律や国際的に受け入れられた基準に違反していないこと
- 具体的な選定基準については、電力制御システム等を利用する部署と連携しつつ決定することが望ましい。

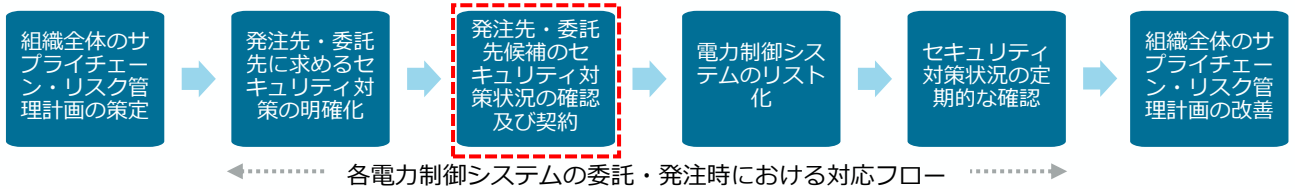
対策のグッドプラクティス

- 契約固有の選定基準は、対象の電力制御システム等の重要度を踏まえて設定する。なお、「経済安全保障推進法」の「特定社会基盤事業者」に該当し、特定重要設備の導入及び重要維持管理等の委託を行う際には、制度によって求められるリスク管理措置を実施する必要があるため、特定社会基盤事業者においては、左記7つすべてのリスク管理措置を選定基準として設定する。
- 重要度は、組織の規模、資産の特性、事業継続に与える影響、サイバー攻撃を受けるリスクを総合的に考慮したうえで設定する。例えば、外部のインターネットと接続するような電力制御システム等の場合、脆弱性を悪用された外部からのサイバー攻撃を防ぐために、発注先・委託先に対し、サービス保証を行うための方法の整備を求める。



3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。

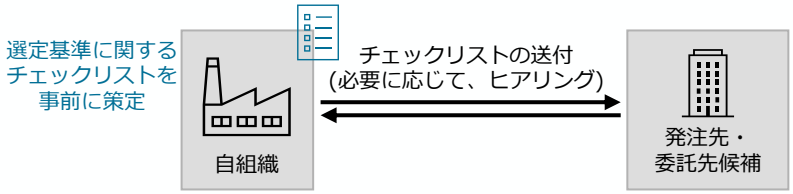


対策実施に関する手引き

- 調達を管理する部署が主体となり、予定している発注先・委託先がセキュリティ対策に関する選定基準を満足しているかを確認するために、発注先及び委託先のセキュリティ対策状況を把握する。
- 発注先・委託先と契約を行う際には、責任範囲の明確化のために、契約書に対し、選定基準として設けたセキュリティ対策を求める内容を記載する。具体的な記述内容については、法務関連部署や発注先・委託先候補と連携しつつ決定することが望ましい。さらに、記述内容の認識合わせのため、発注先・委託先と打ち合わせ等ですり合わせを実施し、議論の内容を議事録などで残すことが望ましい。

対策のグッドプラクティス

- 電力制御システムのセキュリティ設計指針や運用指針を組織全体で定め、その指針を発注先・委託先にも共有することで、サプライチェーン全体のセキュリティ対策レベルを向上する。
- 組織で定めた選定基準に関するチェックリストを策定し、発注先・委託先候補の回答を求める。発注先・委託先候補の回答結果を踏まえ、発注先・委託先候補のセキュリティ対策状況を確認する。必要に応じて、ヒアリングでの追加確認を実施する。



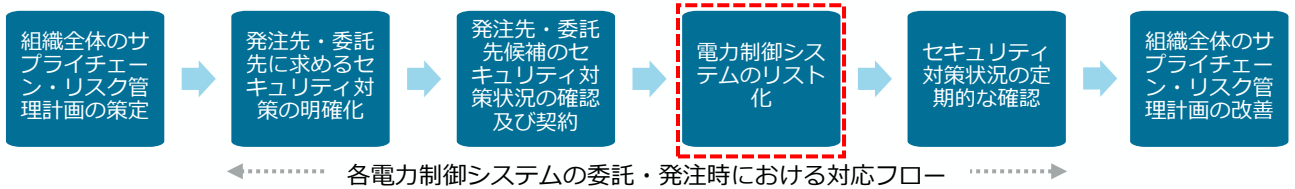
- 選定基準として設けたセキュリティ対策を契約書に明記する際、以下のような条項を設定する。

✓ 【インシデント発生時の連絡の要求】本調達に係る業務の遂行において情報セキュリティが侵害された場合又はそのおそれがある場合には、速やかに当社に報告すること。

✓ 【業務の再委託等に関する制限】業務を再委託する場合、事前に当社の承認を得ること。さらにその際、再委託先のセキュリティ対策が当社の基準に適合していることを証明すること。

3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。



対策実施に関する手引き

- 電力制御システム等の開発・製造、若しくは運用・保守に関する業務委託を実施した際には、当該の電力制御システム等に関する情報及び関係する発注先・委託先の情報を記録することで、電力制御システム等におけるサプライチェーンの依存関係を把握する。

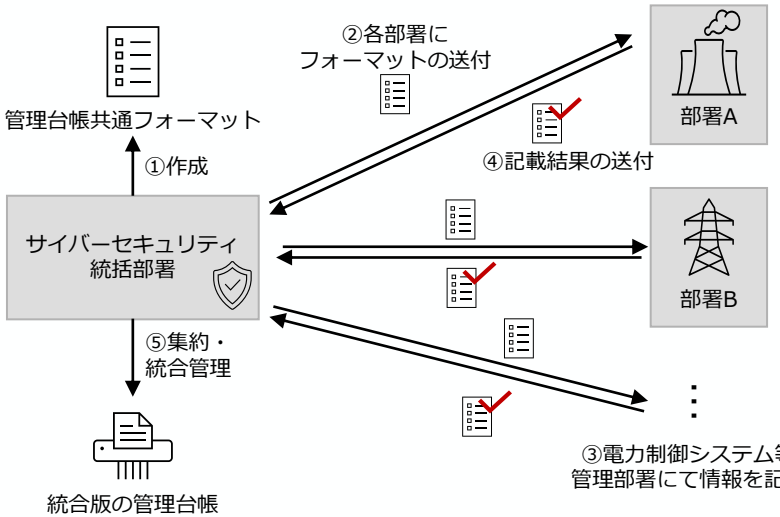
- 記録の実施の際には、統一的な管理台帳を作成すると良い。管理台帳には以下の情報を記載することが想定される。
  - ✓ 電力制御システム等が用いられる業務の分類
  - ✓ 電力制御システム等の名称
  - ✓ 利用範囲（部署名、利用者名など）
  - ✓ 電力制御システム等を開発・製造する発注先・委託先の名称
  - ✓ 電力制御システム等を運用・保守する発注先・委託先の名称
  - ✓ 管理部署及び管理責任者
  - ✓ システム構成
  - ✓ 電力制御システム等が接続する自組織以外の通信回線の種別
  - ✓ 電力制御システム等の利用目的

- 管理台帳については、最低限、年に一回、見直しを行い、内容に変更があった場合には、記載内容の修正を行う。

対策のグッドプラクティス

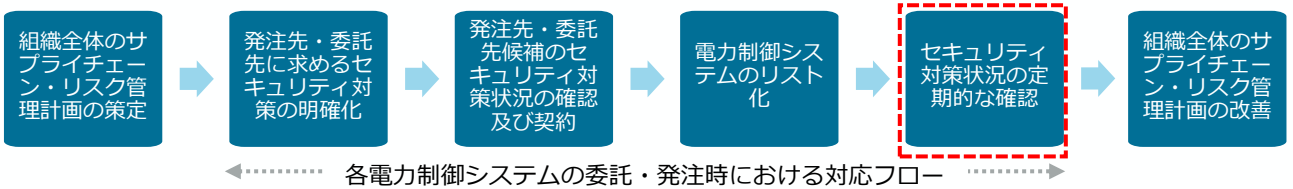
- 管理台帳について、記載事項の統一及び管理の平易化のために、組織全体で共通のフォーマットを用意する。

- 大規模な事業者において効率的に管理台帳に記載・管理するために、まず、電力制御システム等の管理を担当している部署にて管理台帳に情報を記載する。そのうえで、組織全体のサイバーセキュリティを統括している部署にて統合版の管理台帳を確認・管理する。



3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。

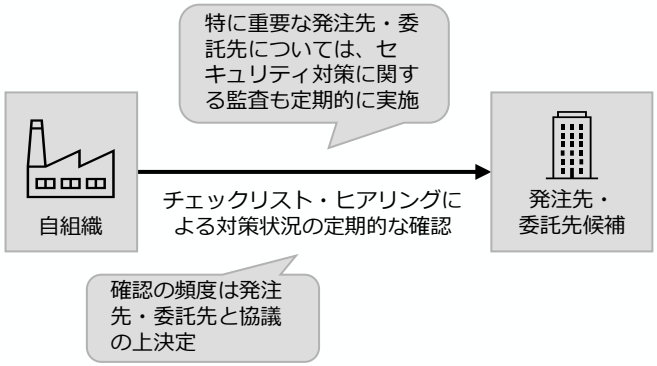


対策実施に関する手引き

- 契約後も、発注先・委託先に対して要求したセキュリティ対策を遵守しているか定期的に確認する。確認及び是正の指示を通して、発注先・委託先もセキュリティ対策の遵守状況を認識することができ、サプライチェーン全体のセキュリティ対策を継続的に向上することができる。
- また、インシデント発生時に迅速に報告できるよう、自組織内に委託先等向けの相談窓口を設置することも想定される。

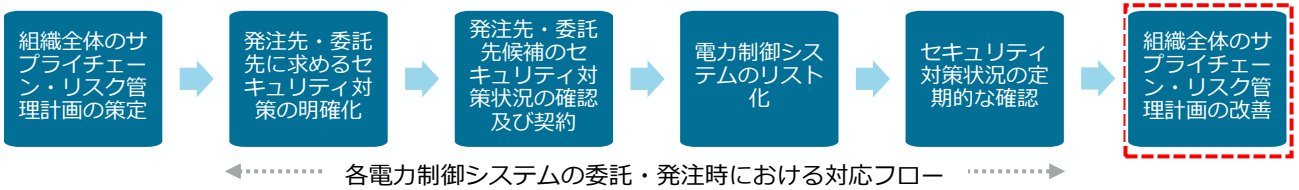
対策のグッドプラクティス

- 発注先・委託先に対して、チェックリストを用いたアンケート調査やヒアリングを実施することで、発注先・委託先に対して要求したセキュリティ対策を遵守しているか定期的に確認する。確認の頻度については、発注先・委託先とあらかじめ協議をしたうえで決定する。
- 特に重要な発注先・委託先については、あらかじめ実施方法を協議したうえで、セキュリティ対策に関する監査を定期的に実施する。



3.1. 「1. サプライチェーン・リスク管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 B) 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 C) 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。



対策実施に関する手引き

- サプライチェーン・セキュリティ対策はPDCAサイクルによる継続的改善が重要である。このために、サプライチェーン・リスク管理計画を定期的に見直す。最低限一年に一度、定期的な見直しを行うことが望まれるほか、サプライチェーン・リスク管理計画に影響を及ぼす事象が発生した際にも見直しを行う。

対策のグッドプラクティス

- 以下の事象が発生した際に、サプライチェーン・リスク管理計画を見直す。

事象	評価観点	見直すべき点
自組織のサプライチェーン上でインシデントが発生した場合	• 対応事項及び担当する部署等の方針 • 全社的な委託先等のセキュリティ対策に関する選定基準 が適切であるか。	インシデントの原因を特定し、再発しないよう、対応事項及び選定基準を見直す。なお、担当部署等が想定した役割を果たしているかも確認し、改善すべき点があれば見直す。
サプライチェーン・リスク管理に関する新たな規制等が発表された場合	• サプライチェーン・リスク管理計画を実施する目的・目標 • 対応事項及び担当する部署等の方針 • 全社的な委託先等のセキュリティ対策に関する選定基準 が適切であるか。	既存のサプライチェーン・リスク管理計画が新たな規制の要求事項をカバーできているかを確認し、改善すべき点があれば見直す。

3.2. 「2. セキュリティ仕様の確認」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 B) 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 C) 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。

対策実施に関する手引き

- 電力制御システム等の調達時においては、発注先と協力しつつ、機能要件及び非機能要件を明確にし、その要件から求められるセキュリティ仕様を策定したうえで、要件定義書を作成する。なお、不正プログラムによる被害を防止するため、不正プログラム対策の管理及び感染防止の機能は要件定義書において明示的に求めることが望まれる。要件定義書に記載するセキュリティ仕様の例は以下のとおり。

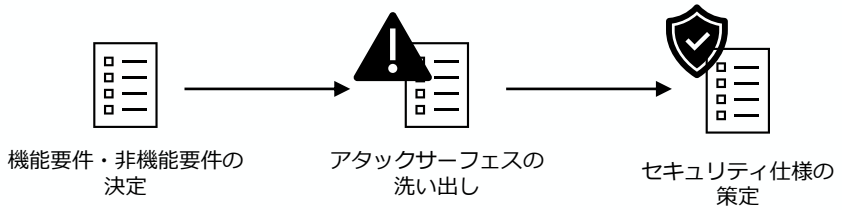
- 通信回線に関する対策
  - 不必要な通信回線からの隔離
  - 不正アクセスの遮断
  - 通信のなりすまし防止
  - サービス不能化の防止
- 構築時及び運用後の脆弱性対策
- 操作ログの収集機能、保存可能な期間、アクセス権限の管理
- 侵入及び不能化の検知
- アカウント管理による利用者の制限
- 機密性・完全性の確保
  - 通信経路上の盗聴防止
  - 保存した情報の機密性及び完全性の確保
- 侵入対策等の物理的保護
- 障害発生時の可用性確保
- 納品時のセキュリティ仕様に関する検収の実施

対策のグッドプラクティス

- 機能要件・非機能要件の決定に際しては、調達する電力制御システム等で「何を実現したいのか」を整理のうえで、それを実現するための機能要件・非機能要件を決定する。必要に応じて、発注先と協議のうえで、目的の達成に向けてセキュリティ仕様が妥当であるか、仕様漏れが存在しないかを確認する。

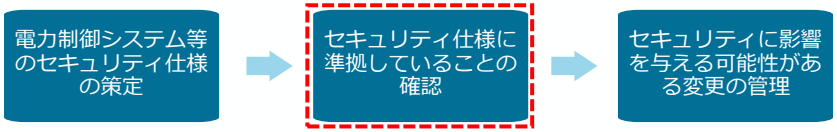
- セキュリティ要件の策定に際して、アタックサーフェスになり得る機能要件及び非機能要件を洗い出す。例えば、当該の電力制御システム等に対して遠隔制御の機能を実装する場合、遠隔制御を行う際に利用する通信回線がアタックサーフェスになり得るため、「通信回線に関する対策」の事項を要件定義書に記載する。

- 自組織で調達する電力制御システム等の典型的な構成を整理し、当該構成に求められるセキュリティ仕様を組織全体で統一化することで、都度のセキュリティ仕様策定の手間を軽減する。



3.2. 「2. セキュリティ仕様の確認」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 B) 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 C) 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。

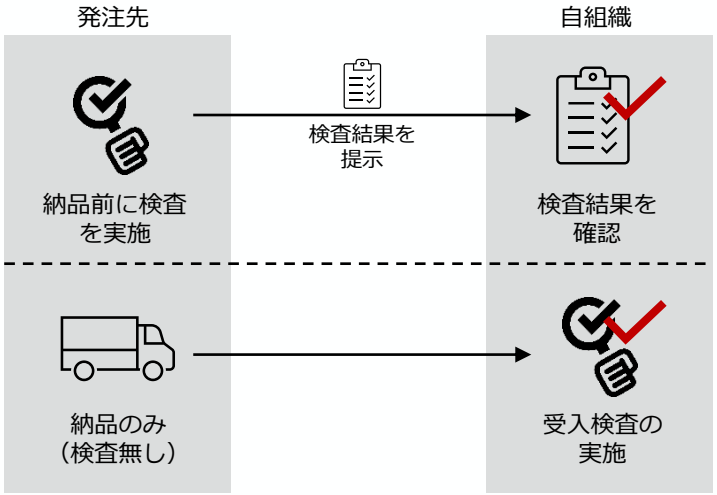


対策実施に関する手引き

- 電力制御システム等が要求したセキュリティ仕様通りに設計、製造されているか確認するため、設計・製造時、出荷時の工程ごとに検査を実施する。
- 検査の実施のために、検査の実施手順や検査基準を定めた手順書等を定めることが望ましい。手順書に記載する事項としては、以下の事項が想定される。
  - ✓ セキュリティ仕様に対する検査方法
  - ✓ 検査を実施するタイミング
  - ✓ 検査の合格基準
  - ✓ 検収不合格の際に発注先に求める対応のプロセス

対策のグッドプラクティス

- 発注先で実施された検査の結果を活用する場合、発注先の検査結果の適正性を評価のうえで、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。
- 自組織で受入検査を実施する場合、要件定義書に記載したセキュリティ仕様の準拠を確認するために必要な具体的な検査方法について、発注先とあらかじめ確認する。



3.2. 「2. セキュリティ仕様の確認」に関する対策の手引き・プラクティス

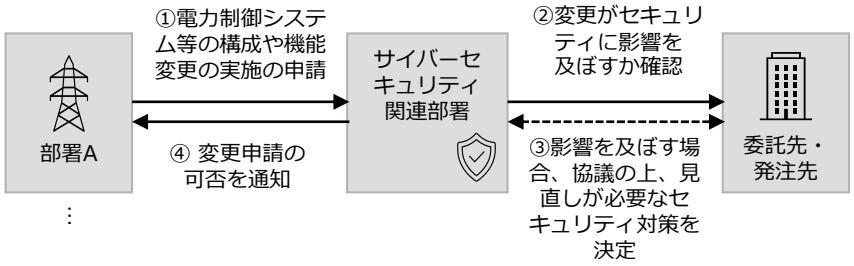
求められるサプライチェーン・セキュリティ対策	A) 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 B) 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 C) 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。

対策実施に関する手引き

- ソフトウェアやファームウェアの更新等により、電力制御システム等の構成や機能変更を実施する場合は、セキュリティ対策への影響を再確認し、必要に応じて、セキュリティ対策の見直しを実施する。
- セキュリティに影響を与える可能性がある変更を適切に管理するために、機能変更時の手順を資料化する。当該手順においては、電力制御システム等の構成や機能変更等が行われる場合に、漏れなくセキュリティ対策への影響を再確認する手順を含めるほか、再確認によりセキュリティ対策の見直しが必要な場合の手順も含める。

対策のグッドプラクティス

- 電力制御システム等の変更を確認・管理するプロセスを組織内に設け、サイバーセキュリティ関連部署において、申請された変更がセキュリティに影響を与える可能性を判断する。
- ソフトウェアやファームウェアの更新等を行う場合、電力制御システム等の構成や機能に変更を及ぼし得るか、事前に委託先・発注先にその影響を確認する。
- 構成や機能の変更に伴いセキュリティに影響を及ぼす場合、委託先・発注先と協議のうえ、見直しが必要なセキュリティ対策を決定する。



3.3. 「3. 機器の適切な管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 機器の管理に関して、機器をライフサイクルを通じて管理し、保護する。

対策実施に関する手引き

- 自組織で保有する機器を起因としたインシデント発生リスクを低減するために、ライフサイクルを通じて適切な管理・保護を行う。このために、機器の運用・管理方法を整備し、文書化する。具体的には、以下を管理する仕組みを整備し、文書化することが想定される。
  - ✓ 機器の選定や設置（保管）場所
  - ✓ 機器の管理者・利用者の登録・変更方法
  - ✓ 機器のデータに関するバックアップ方法
  - ✓ 機器において故障が生じた場合の対応方法
  - ✓ 機器の廃棄方法、保存データの抹消方法
  - ✓ 運用・管理方法に関する見直し・変更の手順

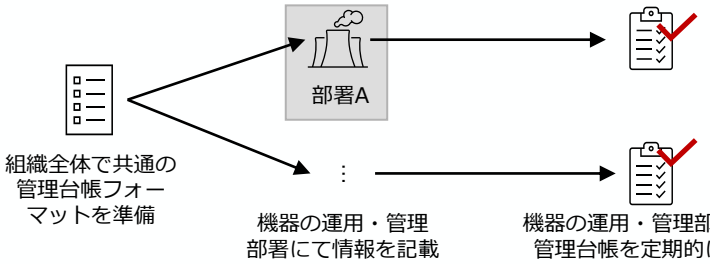
- 機器の管理台帳を作成することも重要である。管理台帳に記載することが想定される情報は以下のとおり。
  - ✓ 機器の管理番号
  - ✓ 機器が用いられる業務の分類
  - ✓ 機器の名称
  - ✓ 利用範囲（部署名、利用者名など）
  - ✓ 機器の設置場所
  - ✓ 機器を開発・製造する委託先等
  - ✓ 機器を運用・保守する委託先等
  - ✓ 管理部署及び管理責任者
  - ✓ 機器が接続する自組織以外の通信回線の種別
  - ✓ 機器の利用目的
  - ✓ 機器のバージョン情報

対策のグッドプラクティス

- 各機器の運用・保守を行う部署が主体となって、現状の運用・管理方法を記載した文書が整備されているかを確認する。文書に不備がある場合には、当該の不備が解消できるよう、運用・管理方法に関する項目を整備する。

- 管理台帳について、記載事項の統一及び管理の平易化のために、組織全体で共通のフォーマットを用意する。また、管理台帳に正確な情報を記載するために、機器の運用・管理を実施している部署等にて、当該機器に関する情報を記載する。

- 管理台帳について、最低限、年に一回、機器の運用・管理を実施している部署等が記載内容の確認を行い、実態と異なる場合には、修正を行う。



- リスク度合いの高い外部記憶媒体（USBメモリ等）の利用を禁じる。やむを得ず利用する必要がある場合には、事前に情報の取扱いに関する実施手順を定めるとともに、データ暗号化機能やマルウェアチェック機能等を有するセキュリティ対策を施した外部記憶媒体の利用に限定する。さらに、利用名簿等に基づき外部記憶媒体の利用者や利用目的を管理する。

3.3. 「3. 機器の適切な管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 機器の管理に関して、機器をライフサイクルを通じて管理し、保護する。

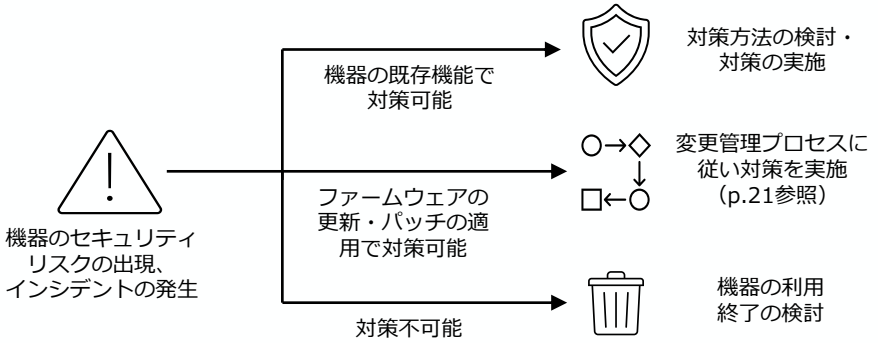
保有する機器の運用・管理方法の整備 → 運用・管理状況の定期的な確認 → 機器の利用終了・廃棄

対策実施に関する手引き

- 機器の運用・管理方法は、定期的な見直しを行う。最低限一年に一度、定期的に見直しを行うことが望まれるほか、新たなセキュリティ上の脅威の出現や当該の機器を起因としたセキュリティインシデントが発生した際にも見直しを行う。
- 機器の運用・管理に係る作業の記録を管理し、運用・管理によって機器の構成や設定情報等に変更があった場合には、定期的な確認に加えて、運用・管理方法の見直しを行う。
- 機器の運用段階で新たな脆弱性を検出した場合、「情報セキュリティ早期警戒パートナーシップガイドライン」を参考に、脆弱性関連情報の届出等の対応を実施する。

対策のグッドプラクティス

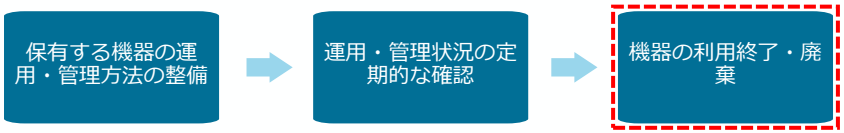
- 利用している機器について、脆弱性の報告等、新たなセキュリティ上のリスクの出現や当該の機器を起因としたセキュリティインシデントが発生した場合には、現状の機器の機能で対策が可能かを発注先に問い合わせ、対応方法を検討する。ファームウェアの更新やパッチの適用によって機器の仕様が変更される場合には、仕様変更後のセキュリティ機能の適切な運用方法も併せて発注先に問い合わせ、運用・管理方法に組み込む。
- ファームウェアの更新やパッチの適用が実施できない場合には、当該の機器の利用終了も検討する。



- 機器の運用・管理の実施において、別の機器との接続といった構成の変更や、設定の変更を行った場合には、当該の構成の変更及び設定の変更がセキュリティ機能の運用方法に影響を及ぼすか確認するために、発注先から提供されたマニュアルを確認するか、発注先に直接問い合わせる。影響があれば、セキュリティ機能の運用方法を見直す。

3.3. 「3. 機器の適切な管理」に関する対策の手引き・プラクティス

求められるサプライチェーン・セキュリティ対策	A) 機器の管理に関して、機器をライフサイクルを通じて管理し、保護する。

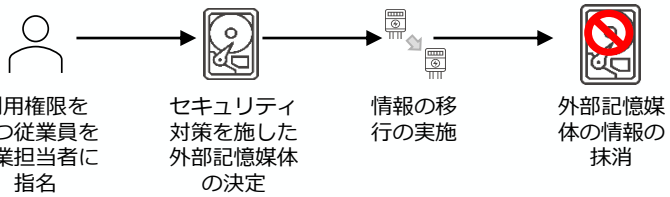


対策実施に関する手引き

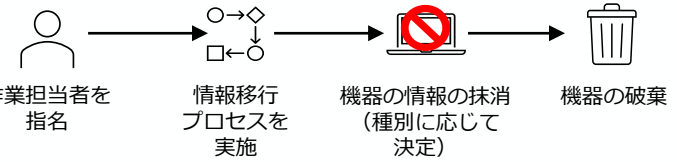
- 機器の利用終了・廃棄に際して、他の機器への情報の移行を実施する際には、移行作業の過程で情報が外部に漏えいすることがないよう、移行する情報を適切に管理する必要がある。
- 廃棄の際には、機器の内部に保存されている情報を適切に抹消する必要がある。廃棄を業務委託する際には、委託先において情報の抹消が適切に行われるよう、抹消方法等について仕様書等に明記し、あらかじめ委託先等と合意しておく必要がある。また、委託先等の抹消作業に関する作業完了の証明を、書面等で受け取ることが望ましい。
- 機器の利用終了・廃棄を行った際には、管理台帳にその旨記載を行う。

対策のグッドプラクティス

- 機器の利用終了・廃棄作業においては、当該の機器の利用権限を持っていた従業員を作業担当者に指名し、当該の担当者のみに作業を行わせることによって、情報の漏えいを防ぐ。なお、情報の移行において外部記憶媒体を利用する場合には、データ暗号化機能やマルウェアチェック機能等を有するセキュリティ対策を施した外部記憶媒体を利用し、移行完了時には情報を適切に抹消する。



- 機器の内部に保存されている情報の抹消方法の決定に際しては、機器の種別に応じて決定する必要がある。例えば、磁気媒体は磁気によって情報を保存しているため磁気破壊による情報の抹消が有効であるが、ソリッドステートドライブは電気信号によって情報を保存しているため、磁気破壊は利用できない。



1. 背景と目的

2. 求められるサプライチェーン・セキュリティ対策

3. 対策の手引き・プラクティス

4. 付録

4.1 用語集

4.2 参考文書

4.1 用語集

用語	説明
ISMS	Information Security Management System（情報セキュリティマネジメントシステム）の略。組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。国際規格ISO/IEC 27001に要求事項が定められている。
ISMS認証	ISMSの要求事項を遵守していることの認証。認証機関による審査を受け、認証基準に適合していると認められることで、事業者等はISMS認証を取得することができる。
PDCA	Plan - Do - Check - Act の略。品質改善や環境マネジメントでよく知られた手法であり、次のステップを繰り返しながら、継続的に業務を改善していく手法の1つのこと。 1.Plan：問題を整理し、目標を立て、その目標を達成するための計画を立てる。 2.Do：目標と計画をもとに、実際の業務を行う。 3.Check：実施した業務が計画どおり行われて、当初の目標を達成しているかを確認し、評価する。 4.Act：評価結果をもとに、業務の改善を行う。
アクセス権限	デバイス上で、プログラムの実行や、データの参照、追加、変更、削除などをできる資格。
インシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
委託先	電力制御システム等に関する保守・管理等の作業を外部委託する際の相手先。
委託先等	委託先、再委託先（別の事業者に委託する再々委託等、多段階の委託が行われる場合の委託先を含む）及び発注先。
外部のデバイス等との接続に係るインターフェース	外部のデバイスと情報の授受を行う際の仕様又はその接続を行う物理的な部分。
可用性	認可された利用者が、必要なときに情報へのアクセス及び使用が可能である特性。[JIS Q 27000:2019]
監査	監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。[JIS Q 27000:2019]
完全性	正確さ及び完全さの特性。[JIS Q 27000:2019]
機器	システムを構成するサーバー、パソコンや可搬型の機器等の端末及びネットワークの構成機器のこと。[電力制御システムセキュリティガイドライン]
機密性	情報にアクセスすることが認可されたものだけがアクセスできる特性。[JIS Q 27000:2019]

4.1 用語集

用語	説明
経済安全保障推進法	経済活動に関して行われる国家・国民の安全を害する行為を未然に防止するため、基本方針の策定及び必要な制度の創設を定めた法律。
再委託先	委託先が再委託を行う際の相手先。
サイバー攻撃	資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2019]
サイバーセキュリティ	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること。[サイバーセキュリティ基本法]
サービス保証	発注先・委託先が提供するサービスの品質について、一定の水準を保証すること。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。本文書では、電力制御システム等の開発や製造に関する一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般の流れを指す。[サイバーセキュリティ戦略]
サプライチェーン・セキュリティ対策	電力制御システム等のサプライチェーン・リスクに対するサイバーセキュリティ上の対策。
サプライチェーン・リスク	電力制御システム等のサプライチェーンにおけるサイバーセキュリティ上のリスク。
サプライチェーン・リスク管理計画	電力制御システム等に関するサプライチェーン・リスクを管理するために定める、全社的な計画。
重要部品	サイバー攻撃等の不正な操作によって電力制御システム等に甚大な影響を及ぼす部品。
情報セキュリティ事象	情報セキュリティの方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。
脆弱性	一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2019]
セキュリティ仕様	電力制御システム等の機能要件に応じて策定されたセキュリティ要件。[電力制御システムセキュリティガイドライン]

4.1 用語集

用語	説明
操作ログ	デバイス等の利用者の操作の履歴。
通信回線	あるデバイスから離れた場所にある別のデバイスまで信号やデータを伝達する物理的な媒体や経路。
通信経路	あるデバイスから離れた場所にある別のデバイスまで信号やデータを伝達する際に利用される論理的な道筋。
電力制御システム	電力の安定供給、電気工作物の保安（公衆安全を含む）の確保に資するために、電気事業の用に供する電気工作物を監視・制御する機能等を具備したシステム。[電力制御システムセキュリティガイドライン]
電力制御システム等	電力制御システム及び電力制御用ネットワークの全体。[電力制御システムセキュリティガイドライン]
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制度	経済安全保障推進法に基づき設立された制度。国が一定の基準のもと、基幹インフラ事業（特定社会基盤事業）・事業者（特定社会基盤事業者）を指定し、国が指定した重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際には、事前に国に届出を行うことを求めている。
任務保証	企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。[サイバーセキュリティ戦略]
発注先	電力制御システム等の発注若しくは開発・製造の依頼を行う際の相手先。
秘密保持条項	委託業務の実施において得た秘密情報について、外部への漏えいや目的外利用がないように秘密保持（守秘）義務を課す条項。
不正アクセス	本来はアクセス権限を持たない者が、デバイスの内部へ侵入する行為。
不正プログラム	デバイスに対して意図的に何らかの被害を及ぼすように作られたプログラム。
ライフサイクル	電力制御システム等の計画・開発・調達・運用・保守・廃止のこと。[電力制御システムセキュリティガイドライン]
リスク	任務保証の考え方を踏まえ、電力の安定供給や電力プラントの安全運用を不確かなものとする自然災害、管理不良、サイバー攻撃や、電力分野を取り巻く環境変化等のこと。[重要インフラのサイバーセキュリティに係る行動計画]

4.2 参考文書

文書名	発行元	概要
電力制御システムセキュリティガイドライン	日本電気協会	電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策について規定した文書。
サイバーセキュリティ戦略	内閣（閣議決定）	政府におけるサイバーセキュリティ施策や実施方針となる戦略文書。
重要インフラのサイバーセキュリティに係る行動計画	内閣官房　内閣サイバーセキュリティセンター	重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画を定めた文書。
重要インフラのサイバーセキュリティに係る安全基準等策定指針	内閣官房　内閣サイバーセキュリティセンター	「重要インフラのサイバーセキュリティに係る行動計画」を踏まえ、重要インフラ分野におけるサイバーセキュリティの確保に向けた取組を整理した指針。
重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引	内閣官房　内閣サイバーセキュリティセンター	「重要インフラのサイバーセキュリティに係る安全基準等策定指針」で示された取組のうち、リスクマネジメントの主要なプロセスやセキュリティ対策が示された手引文書。
政府機関等のサイバーセキュリティ対策のための統一基準	内閣官房　内閣サイバーセキュリティセンター	国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組み。情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定。
政府機関等の対策基準策定のためのガイドライン	内閣官房　内閣サイバーセキュリティセンター	「政府機関等のサイバーセキュリティ対策のための統一基準」の遵守事項を満たすためにとるべき基本的な対策事項の例示と、対策基準の策定及び実施に際しての考え方等を解説したガイドライン。
情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	内閣官房　内閣サイバーセキュリティセンター	政府機関における情報システムの調達仕様書に記載するセキュリティ要件の策定方法を解説した文書。
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	内閣府	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制度の基本指針を示した文書。
電気事業における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	経済産業省	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制度について、電気事業者が留意すべき事項を解説した文書。

4.2 参考文書

文書名	発行元	概要
サイバーセキュリティ経営ガイドライン	経済産業省	大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するための原則や重要項目を示したガイドライン。
制御システムのセキュリティリスク分析ガイド	独立行政法人情報処理推進機構（IPA）	制御システムのセキュリティを抜本的に向上させるのに重要な位置づけとなるセキュリティリスク分析を事業者が実施できるようにするためのガイド。
組織における内部不正防止ガイドライン	IPA	企業やその他の組織において必要な内部不正対策を効果的に実施可能とすることを目的としたガイドライン。
実務者のためのサプライチェーンセキュリティ手引書	IPA	サプライチェーン・セキュリティに携わる実務者のサポートを目的とした手引書。
情報セキュリティ早期警戒パートナーシップガイドライン	IPA、JPCERT コーディネーションセンター（JPCERT/CC）等	国内でソフトウェア等の脆弱性関連情報を適切に流通させるために作られている枠組みである「情報セキュリティ早期警戒パートナーシップ」に関して、関係者（発見者、IPA及びJPCERT/CC、製品開発者、ウェブサイト運営者）に推奨する行為をまとめたガイドライン。
サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて	経済産業省、公正取引委員会	中小企業等におけるサイバーセキュリティ対策を支援するための施策とともに、取引先への対策の支援・要請に係る関係法令の適用関係を示した指針。
NIST Cybersecurity Framework 2.0	米国立標準技術研究所（NIST）	組織がセキュリティリスクを管理する際の基準及びガイドライン、また参考になるベストプラクティスを定めたフレームワーク。
Good Practices for Supply Chain Cybersecurity	欧州ネットワーク情報セキュリティ機関（ENISA）	大企業、重要インフラ事業者、公共サービスを対象とした、サプライチェーン・セキュリティ対策のプラクティスをまとめた文書。
Supply chain security guidance	英国国家サイバーセキュリティセンター（NCSC）	プライチェーン・セキュリティ対策のガイドライン。サプライチェーンを効果的に管理・監督するための12の原則を提案した文書。

4.2 参考文書

文書名	発行元	概要
How to assess and gain confidence in your supply chain cyber security	英国NCSC	中規模から大規模の組織がサプライチェーン・セキュリティ対策を行う際の手順を示した文書。
Best Practices in Cyber Supply Chain Risk Management	米国NIST	対象分野を指定しない汎用的なサプライチェーン・セキュリティ対策のプラクティス集。
Securing Small and Medium-sized Business Supply Chains -A resource handbook to reduce information and communication technology risks-	米国サイバーセキュリティ・インフラセキュリティ庁（CISA）	中小企業がサプライチェーン・リスクの管理を行う際に留意すべき事項をまとめた文書。
Information and Communications Technology Supply Chain Risk Management (SCRM) in a Connected World	米国CISA	ICT製品を調達する際に留意すべきサプライチェーン・リスクと、その管理方法をまとめた文書。
NISTIR 8259シリーズ	米国NIST	IoT機器に関する製造業者と、それを支援するサードパーティ事業者において、IoT機器を構想、設計、開発、テスト、販売、サポートする際のガイダンスを提供した文書。本編であるNISTIR 8259を補完する位置づけであるNISTIR 8259A及び8259Bでは、製造業者が考慮すべき技術的機能及び非技術的なサポート活動をそれぞれ示している。
Supply Chain Cybersecurity Principles	米国エネルギー省（DoE）	エネルギー関連事業者、当該事業者にICSを納入するベンダーを対象とした、サプライチェーン・セキュリティ対策を行う際のプラクティスをまとめた文書。