経済産業省

資料４－１

公表用

サプライチェーン・リスクへの対応と リスク点検ツールの活用について

2026年2月12日

資源エネルギー庁　電力基盤整備課

目次

目次

新たなサイバーセキュリティ政策の全体像及び今後の方向性

- NCOをはじめ関係省庁との連携の下、サイバーセキュリティ市場における**需要拡大と供給力強化に向けた取組**や、**国際的な制度調和と国内での調達要件化促進**、**サイバー情勢分析能力強化**を図っていく。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 我が国の半導体関連産業におけるセキュリティ対策水準の向上を通じた競争力確保
- 地域における中小企業支援の拡大（サイバーセキュリティお助け隊サービスの普及促進等）
- SCS評価制度の構築（対策水準の可視化）　等

⇒政府調達・補助金の要件化等を通じた実効性強化

②セキュア・バイ・デザインの実践

- IoT製品におけるJC-STARの普及、国際制度調和の調整
- SBOM（Software Bill of Materials）の活用促進、安全なソフトウェアの開発に向けた指針の整備
- サイバーインフラ事業者の責務の明確化

⇒国際連携を前提とした制度構築と政府調達等要件化を通じた制度の普及

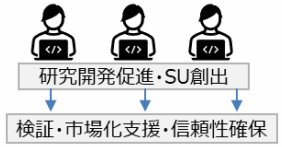
③政府全体でのサイバーセキュリティ対応体制の強化

- IPAのサイバー情勢分析能力強化
- 改正保安３法を踏まえたサイバー事故調査体制の構築
- サイバー攻撃技術情報の共有促進　等

⇒官民のサイバー状況把握力・対処能力向上と関係省庁との連携

④サイバーセキュリティ供給能力の強化

- サイバーセキュリティ産業振興のための政策パッケージの推進
- 先進的サイバー防御機能・分析能力の強化
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）、若手人材発掘機会（セキュリティ・キャンプ）の拡大　等



IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

⇒セキュリティ市場の拡大に向けたエコシステムの構築

電力分野のサイバーセキュリティ対策の取組

事業者で区分されるガイドライン等

区分	名称	概要【所管・発行主体】	発電事業者	送配電事業者	特定卸供給事業者	小売電気事業者
法令	サイバーセキュリティ基本法（重要インフラのサイバーセキュリティに係る行動計画）	重要インフラ事業者に指定された者に、サイバーセキュリティ確保の取組やインシデント発生時の政府への情報連絡等を求める【NCO】	○	○	ー	ー
法令	サイバー対処能力強化法	特定社会基盤事業者に指定された者に、電子計算機を導入する際の資産届出やインシデント報告、協議会への参加等を求める。【NCO】	○ 50万kW以上	○ 全社指定	○ 50万kW以上	ー
法令	特定卸供給に係るサイバーセキュリティ確保の指針	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示した指針。事業届出の際には、本指針に基づく対策実施状況を記載する必要がある。【エネ庁】	ー	ー	○	ー
契約	系統連系技術要件（託送供給等約款）	系統連系する発電設備、及び高圧以上の需要設備に求められるセキュリティ対策を規定。また、2027年度以降、系統に接続する太陽光発電・蓄電池に対してJC-STAR★1を取得した機器の使用を要件化予定。【各一般送配電事業者】	○ 発電設備	ー	ー	○ 需要設備
その他	小売電気事業者のためのサイバーセキュリティ対策ガイドラインVer1.0	小売電気事業者が情報システムを利活用し、そのサービスの品質を高めていくに当たって、効果的なサイバーセキュリティ対策を推進するための指針。【エネ庁】	ー	ー	ー	○
その他	エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドラインVer3.0	エネルギー・リソース・アグリゲーション・ビジネス（ERAB）に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を記載。【エネ庁・IPA】	○	○	○	○
その他	リスク点検ツール	各事業者において、リスク点検項目に対する対応状況を入力し、セキュリティ対策状況の可視化・自己診断に使用。【エネ庁】	○	○	○	○

電力分野のサイバーセキュリティ対策の取組（ガイドライン等）

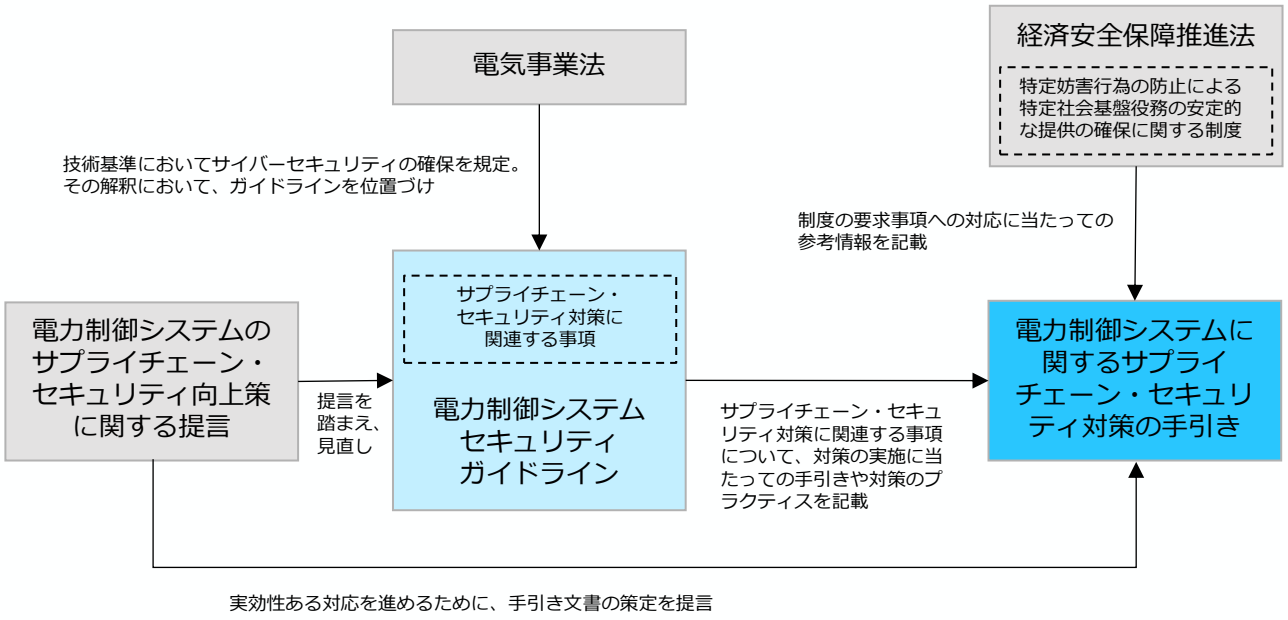
電気工作物で区分されるガイドライン等

区分	名称	概要【所管・発行主体】	電気事業の用に供する電気工作物	自家用電気工作物（発電事業）	自家用電気工作物（発電事業以外）	一般用電気工作物
法令	電気事業法第42条の保安規程（電気事業法施行規則第50条）	事業用電気工作物の設置者は、その設置の際に、当該設備のサイバーセキュリティ確保に関する取組を保安規程に定め、主務大臣に届け出て、その内容を遵守する。【経産省】	○	○	○	ー
法令	電力制御システムセキュリティガイドライン（電気設備の技術基準の解釈第37条の2）	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の要求事項について規定。【日本電気技術規格委員会】	○	○	ー	ー
法令	電力制御システムのサプライチェーン・セキュリティ対策の手引き	「電力制御システムセキュリティガイドライン」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・促進するための手引き文書。【エネ庁】	○	○	ー	ー
法令	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）（電気設備の技術基準の解釈第37条の2）	自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、設置者が実施すべきセキュリティ対策の要求事項を規定【経産省】	ー	ー	○ 小規模事業用電気工作物を除く	ー

目次

電力制御システムのサプライチェーン・セキュリティ対策の手引きの概要

- **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文書**として、**2025年6月**に資源エネルギー庁より公開。
- **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ライクル全般のサプライチェーンに関わる事業者のリスク**に対応するべく、事業者の参考となる情報をまとめたもの。



目次

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

（参考）手引きより抜粋

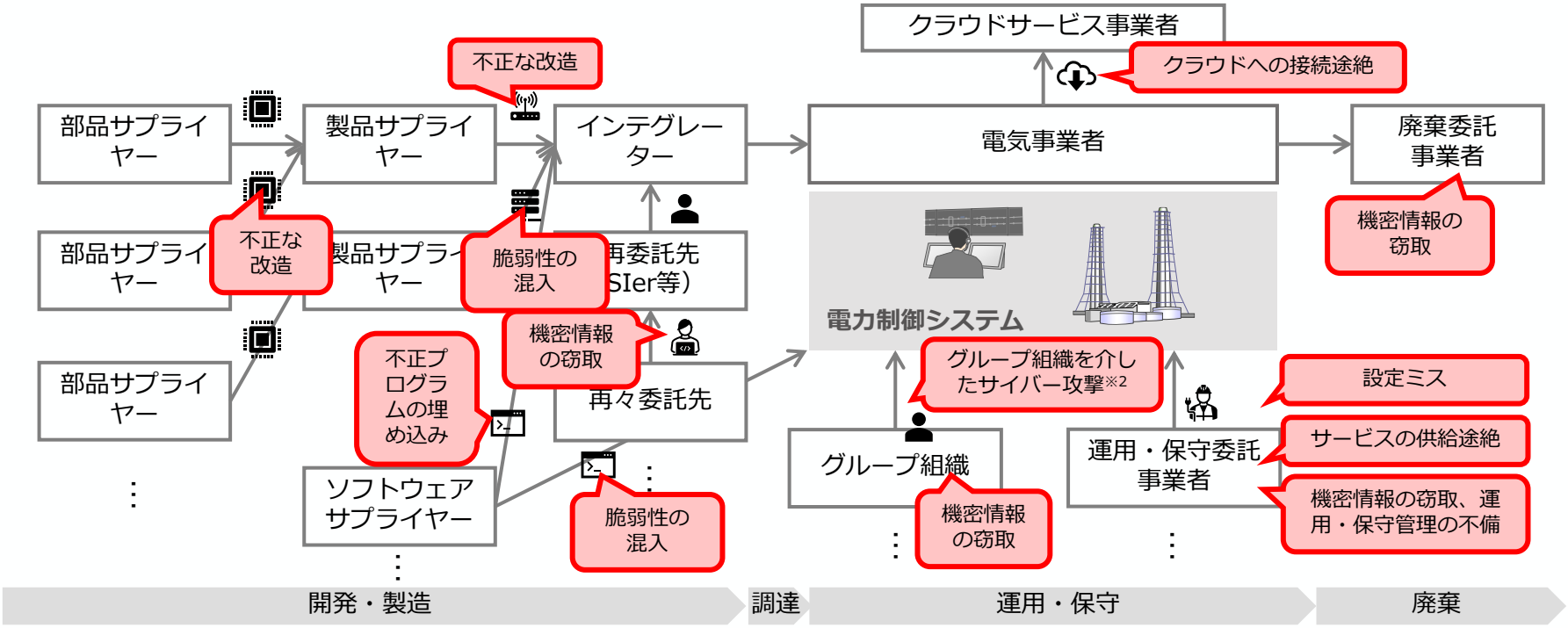
1.2. 本文書におけるサプライチェーン・リスク

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

（参考）手引きより抜粋

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。**

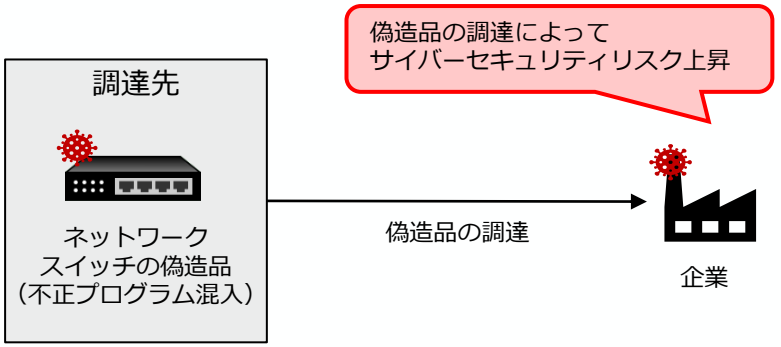
重要インフラ事業者である電気事業者においては、電力安定供給のために適切なサプライチェーン・セキュリティ対策を講じる必要があるところ、**経営層は、サプライチェーン・リスクに対処するために適切なリソース配分と体制の整備を行う必要がある。**

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

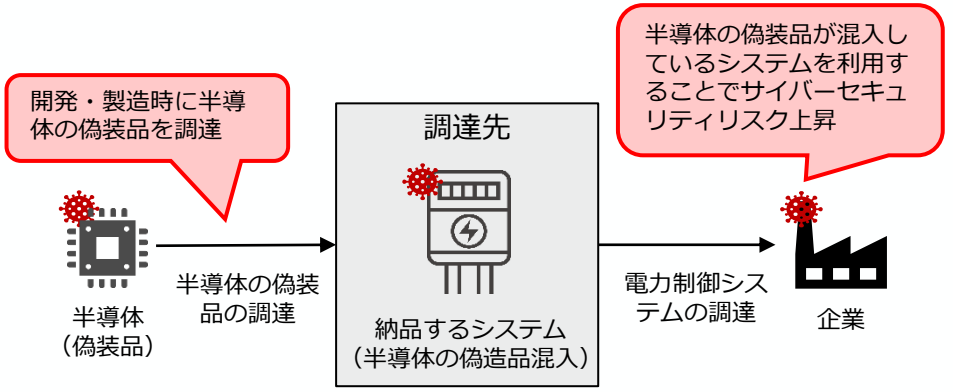
(1) ネットワークスイッチの偽造品の流通

- 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。



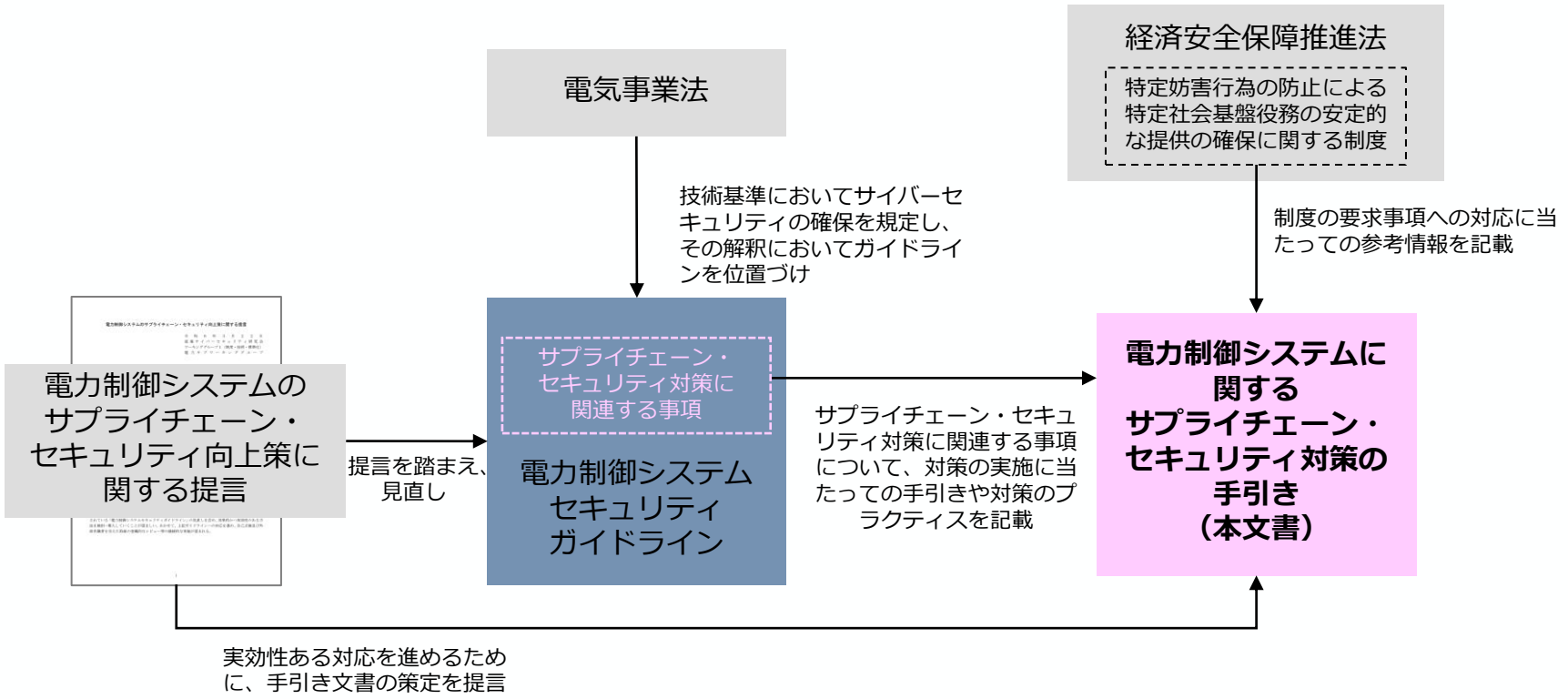
F-Secure, THE FAKE CISCO https://labs.withsecure.com/content/dam/labs/docs/2020-07-the-fake-cisco.pdf
ERAI, 2023 Annual Report https://www.erai.com/erai_blog/3183/_2023_annual_report
EUROPOL, Intellectual Property Crime Threat Assessment 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20ass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

（参考）手引きより抜粋

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

（参考）手引きより抜粋

1.5. 主な対象読者・活用方法

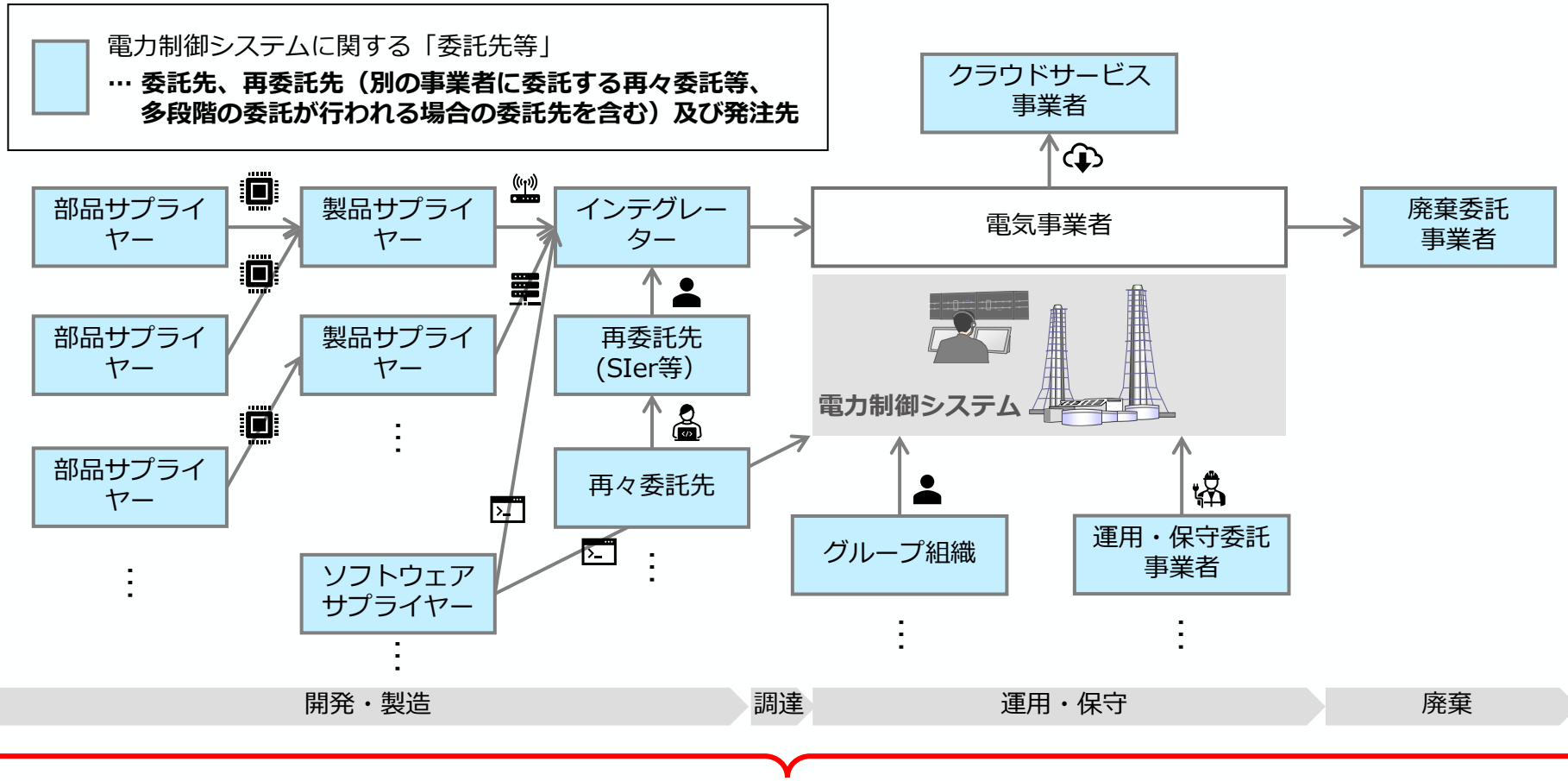
本文書は、**電力制御システムを運用する電気事業者**のほか、**電力制御システムに関する「委託先等」**を主な対象とする。
当該事業者のうち、特に以下の部門及び関係者での活用が期待される。

	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。

（参考）手引きより抜粋

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

（参考）手引きより抜粋

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

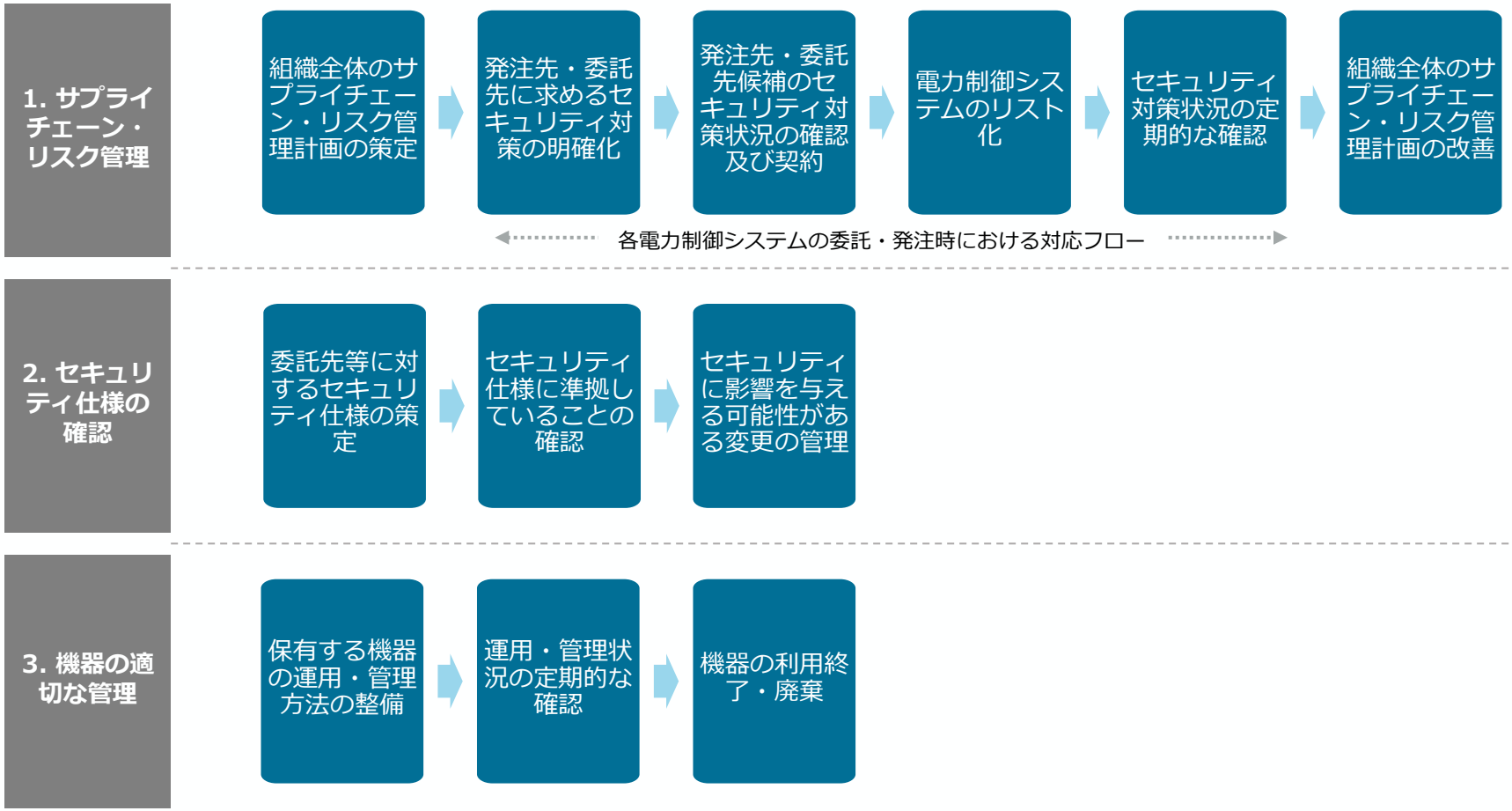
(参考文書)
電力SWG, 電力制御システムのサプライチェーン・セキュリティ向上策に関する提言 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf

（参考）手引きより抜粋

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。

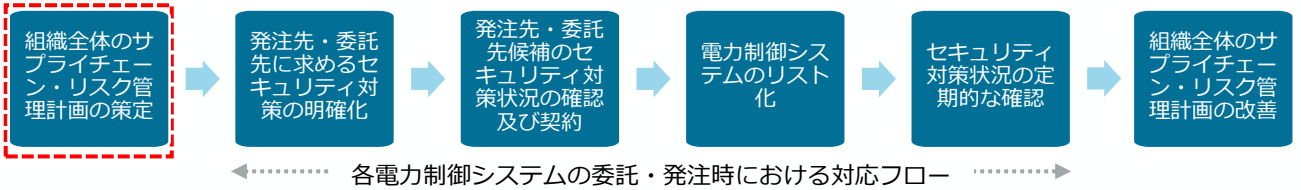
本文書では、各プロセスにおける具体的な対策の手引きや対策に関するグッドプラクティスを提供する。



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

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

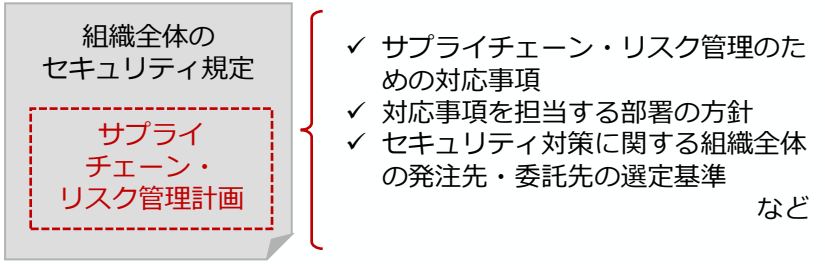
- まず、電力制御システム等のサプライチェーン・リスクを管理するための自組織内の計画を策定する。サプライチェーン・リスクに限定されないリスク管理計画がすでに存在する場合、当該計画に含める形で策定することが効果的である。サプライチェーン・リスク管理計画には以下の事項を含めることが想定される。
  - ✓ サプライチェーン・リスク管理のための対応事項
  - ✓ 対応事項を担当する部署の方針
  - ✓ セキュリティ対策に関する組織全体の発注先・委託先の選定基準

- 「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。

目次

リスク点検ツールの概要

- **電気事業者を主な対象として、過大なコストをかけずに簡易的にリスク点検ができる**よう、**「電力システムにおけるサイバーセキュリティリスク点検ガイド」及び「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を開発**し、**2024年3月に公表**した。
- 可視化ツールは、**電力広域的運営推進機関（OCCTO）のセキュリティ自己診断**においても活用されている。

リスク点検ツールの構成

リスク点検ツール

電力システムにおけるサイバーセキュリティリスク点検に関するガイド

事業者が、自社の対策状況の確認やリスク評価に当たって活用できるガイド。具体的には以下の目次構成を設定する。

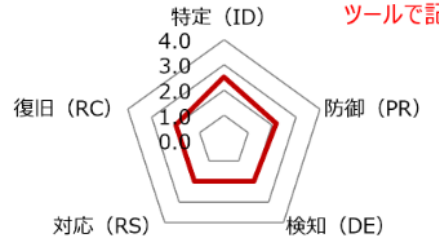
1. 背景・目的
2. 本ガイド・対策状況可視化ツールの構成
3. 本ガイド・対策状況可視化ツールの対象
4. 本ガイド・対策状況可視化ツールの想定活用方法
5. リスク点検項目・対策を怠った場合のリスク
6. リスク点検結果を踏まえた対策の改善方針
7. 参考文書
8. 用語集

＋

電力システムにおけるサイバーセキュリティ対策状況可視化ツール

各事業者がリスク点検項目に対する対応状況を入力することで、組織の対策状況を可視化する。ヒアリング結果を踏まえ、Excel形式にて作成する。

リスク点検項目に対する対応状況を、可視化ツールで記載

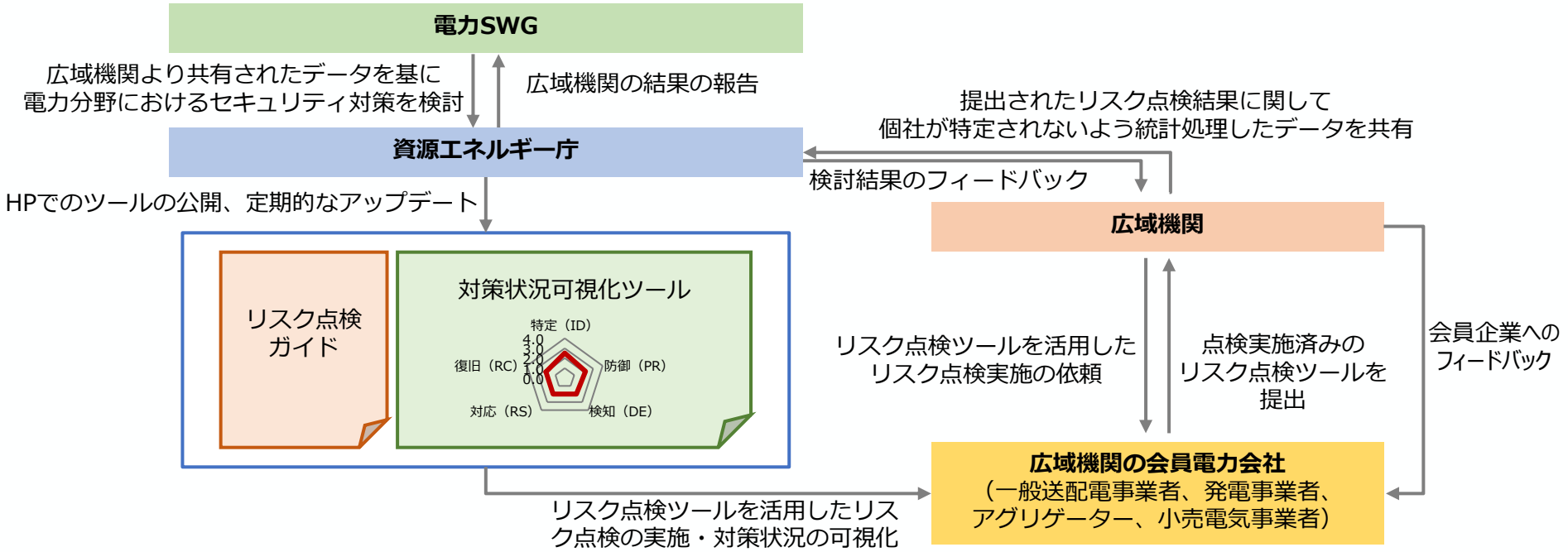


（参考）広域機関の自己診断に関する取組との連携

第16回電力SWG
資料を一部修正

- 昨年度より、広域機関のセキュリティ自己診断の取組において、リスク点検ツールを活用。
- 広域機関では、公開されたリスク点検ツールを参照する形式でリスク点検の実施を会員企業に依頼し、会員企業は、エネ庁HPに掲載されたツールに基づきリスク点検を実施し、実施結果を広域機関に提出。
- 会員企業のリスク点検結果は、広域機関により個社が特定されないよう統計処理した上で、資源エネルギー庁に共有いただいた。
- 引き続きより多くの事業者に活用いただくことで、電力分野全体でのサイバーセキュリティ対策のレベルを底上げしていくことが望まれる。

リスク点検ツールの広域機関との連携スキーム



（参考）リスク点検項目の概要

第16回電力SWG
資料を一部修正

- リスク点検ツールの具体的なリスク点検項目について、国内外の事業者において広く活用され、電事連が電力10社を対象に実施したリスク評価でも活用されたNISTのCybersecurity Framework ver1.1（NIST CSF）を参考に整理。
- NIST CSFでは、5つのセキュリティ機能（特定、防御、検知、対応、復旧）に対し、機能の詳細を定めた23のカテゴリー、108のサブカテゴリーが定義されているため、本リスク点検ツールでは108のサブカテゴリーをリスク点検項目として設定した。

機能	カテゴリー		サブカテゴリー数
特定(ID)	ID.AM	資産管理	6
	ID.BE	ビジネス環境	5
	ID.GV	ガバナンス	4
	ID.RA	リスクアセスメント	6
	ID.RM	リスク管理戦略	3
	ID.SC	サプライチェーンリスクマネジメント	5
防御(PR)	PR.AC	アクセス制御	7
	PR.AT	意識向上及びトレーニング	5
	PR.DS	データセキュリティ	8
	PR.IP	情報を保護するためのプロセス及び手順	12
	PR.MA	保守	2
	PR.PT	保護技術	5

機能	カテゴリー		サブカテゴリー数
検知(DE)	DE.AE	異常とイベント	5
	DE.CM	セキュリティの継続的なモニタリング	8
	DE.CP	検知プロセス	5
対応(RS)	RS.RP	対応計画	1
	RS.CO	伝達	5
	RS.AN	分析	5
	RS.MI	低減	3
	RS.IM	改善	2
復旧(RC)	RC.RP	復旧計画	1
	RC.IM	改善	2
	RC.CO	伝達	3

NIST CSFの各サブカテゴリーを、リスク点検ツールにおけるリスク点検項目として設定

【サブカテゴリーに基づくリスク点検項目の例】

PR.PT-1：監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。(ログの取得を実施している。)

自己診断における回答内容について

- 今年度のセキュリティ自己診断では、リスク点検ツールのリスク点検項目のうち、**過年度の自己診断の対策カテゴリー※を参考に抽出した68項目のみの回答を依頼**した。
  ※サイバーセキュリティ経営ガイドラインをベースに設定したカテゴリー
- **各リスク点検項目について、0～4の5段階で対策状況を回答**いただいた。

対策カテゴリーとカテゴリーごとのリスク点検項目数

対策カテゴリー	リスク点検ツールにおける点検項目数
１：情報セキュリティリスクの認識、組織全体での対応方針の策定	3
２：情報セキュリティリスク管理体制の構築	2
３：情報セキュリティ対策のための資源（予算、人材等）確保	5
４：情報セキュリティリスクの把握とリスク対応に関する計画の策定	13
５：情報セキュリティリスクに対応するための仕組みの構築	24
６：情報セキュリティ対策におけるPDCAサイクルの実施	1
７：インシデント発生時の緊急対応体制の整備	10
８：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	1
９：電力広域的運営推進機関提供の情報システムを利用する際のクライアント証明書の管理について	2
１０：クライアント証明書をインストールしたPCの管理について	2
１１：広域機関システム、スイッチング支援システム、容量市場システムのユーザID,パスワードの管理について	2
１２：需要者や発電設備設置者等の個人情報の管理について	3

スコアの定義

スコア	定義
0	対策項目に対応していない
1	対策項目の一部対応している
2	対策項目に概ね対応している
3	対策項目に対応している
4	対策項目に対応したうえで、見直しも行われている