資料７－１

電力システムにおけるサイバーセキュリティ リスク点検ツールについて

2024年 2月 1日

リスク点検ツールの必要性・作成状況

- サイバーセキュリティ対策の継続的改善・高度化に向けては、「電力制御システムセキュリティガイドライン」にも記載のとおり、**PDCAサイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスが重要**となるが、過年度事業における調査によると、対策を実施している事業者の割合と比較して、**定期的な対策状況の評価（リスク点検）や継続的な対策改善を実施している事業者は限定的**であった。
- 併せて、過年度調査では、電力システムに関連する様々なプレイヤーが**過大なコストをかけることなく簡易的にリスク点検ができるようなツール（チェックリスト等）の必要性が提示された**。
- このような議論を踏まえ、昨年度の事業において、コストを抑えて簡易的にリスク点検ができる**「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」の案を作成**した。
- 今年度、**電気事業者による試行利用を通じてリスク点検ツールの課題等を抽出**するとともに、**試行利用結果を踏まえてツールの改善を行い、リスク点検ツールの正式公開を行う**。また、**リスク点検ツールの正式公開にあたり、リスク点検ツールの位置づけや普及促進策についても検討を行う**。

【参考】リスク点検ツールの構成案

- リスク点検ツールは、**「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（参考資料1）」と「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（参考資料2）」によって構成**する。
- ガイドは、国内電気事業者において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文書とし、**リスク点検項目を示しつつ、リスク点検結果を踏まえた対策の改善方針も示す。**
- 対策状況可視化ツールは、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簡易に組織の成熟度や対策状況を可視化できるツール**とし、Excel形式にて作成する。

リスク点検ツールの構成案

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。

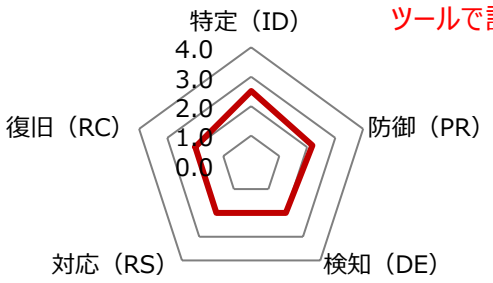
1. 背景・目的
2. 本ガイド・対策状況可視化ツールの構成
3. 本ガイド・対策状況可視化ツールの対象
4. 本ガイド・対策状況可視化ツールの想定活用方法
5. リスク点検項目・対策を怠った場合のリスク
6. リスク点検結果を踏まえた対策の改善方針
7. 参考文書
8. 用語集

＋

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】リスク点検ツールの対象事業者

- リスク点検ツールの対象事業者について、一般送配電事業者については電事連によるリスクアセスメントが推進されているところ、その他の**①発電事業者、②小売電気事業者、③アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）、④自家用電気工作物設備設置者の4区分を主な対象**とする。
- 4区分のうち、大手事業者の多くはリスク点検を既に定期的に実施しているところ、本事業で開発する**リスク点検ツールでは、中小事業者をはじめとするこれまでリスク点検を実施してこなかった事業者をメインスコープ**とし、当該事業者における簡易的かつ効率的なリスク点検を支援する内容とする。

リスク点検ツールの対象事業者

以下の4区分の事業者のうち、中小事業者をはじめとする
これまでリスク点検を実施してこなかった事業者を主な対象とする。

① 発電事業者

② 小売電気事業者

③ アグリゲーター
（アグリゲーションコーディネーター及びリソースアグリゲーター）

④ 自家用電気工作物設備設置者

【参考】リスク点検項目の概要

- **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（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**する。

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
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。)

PR.PT-2：リムーバブルメディアは、保護され、その使用がポリ シーに従って制限されている。(外部記憶媒体をルールに則って管理している。)　等

１．リスク点検ツールの正式公開に向けた取組

2.　リスク点検ツールの普及展開・位置づけについて

試行利用の結果

- リスク点検ツールの正式公開に向け、ツールの課題を抽出することを目的に、電力会社3社に協力いただき、リスク点検ツール案に関する試行利用を実施いただいた。
- 試行利用後、リスク点検ツールの記入時間・難易度、点検項目の内容、ツールの活用方法・メリット・普及展開等についてのアンケートに回答いただいた。
- **リスク点検ツールに対して概ね好意的な意見**が多く、**社内のセキュリティ対策状況確認のコストダウンや外部事業者のセキュリティ対策確認の効率化等のメリットについて確認**できた。

	会社1 （発電事業者・アグリゲーター）	会社2 （小売電気事業者）	会社3 （小売電気事業者・アグリゲーター）
記入時間	2週間～1カ月 （実質時間としては5時間程度）	2週間～1カ月 （実質時間としては15時間程度）	1週間以上2週間未満 （実質時間としては10時間程度）
難易度	適切	難しい	難しい
回答に必要なスキル	応用情報技術者試験程度	情報処理安全確保支援士程度	情報セキュリティマネジメント試験程度
項目数	比較的多い	とても多い	とても多い
項目内容・リスク	分かりやすい	どちらでもない	どちらでもない
達成基準	分かりやすい	分かりづらい	どちらでもない
メリット	• リスク点検の外注費用を抑えられる。 • 本ツールを活用することでVPP事業でも継続的なリスク点検を実施することが可能である。	• より細かな視点でセキュリティ対策をチェックすることができる。	• リスク点検項目が細かく、想定されるリスクもわかりやすい。 • 自社のセキュリティ対策方針作成及びシステムベンダーへのセキュリティ対策に活用可能できる。

試行利用を踏まえたリスク点検ツールの改善

- 試行利用後に事業者から指摘を受けた以下の6点について、以下に示す方針のとおりに修正した。
- 試行利用を踏まえて修正した「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」と「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」はそれぞれ資料7-2と資料7-3に示すとおり。

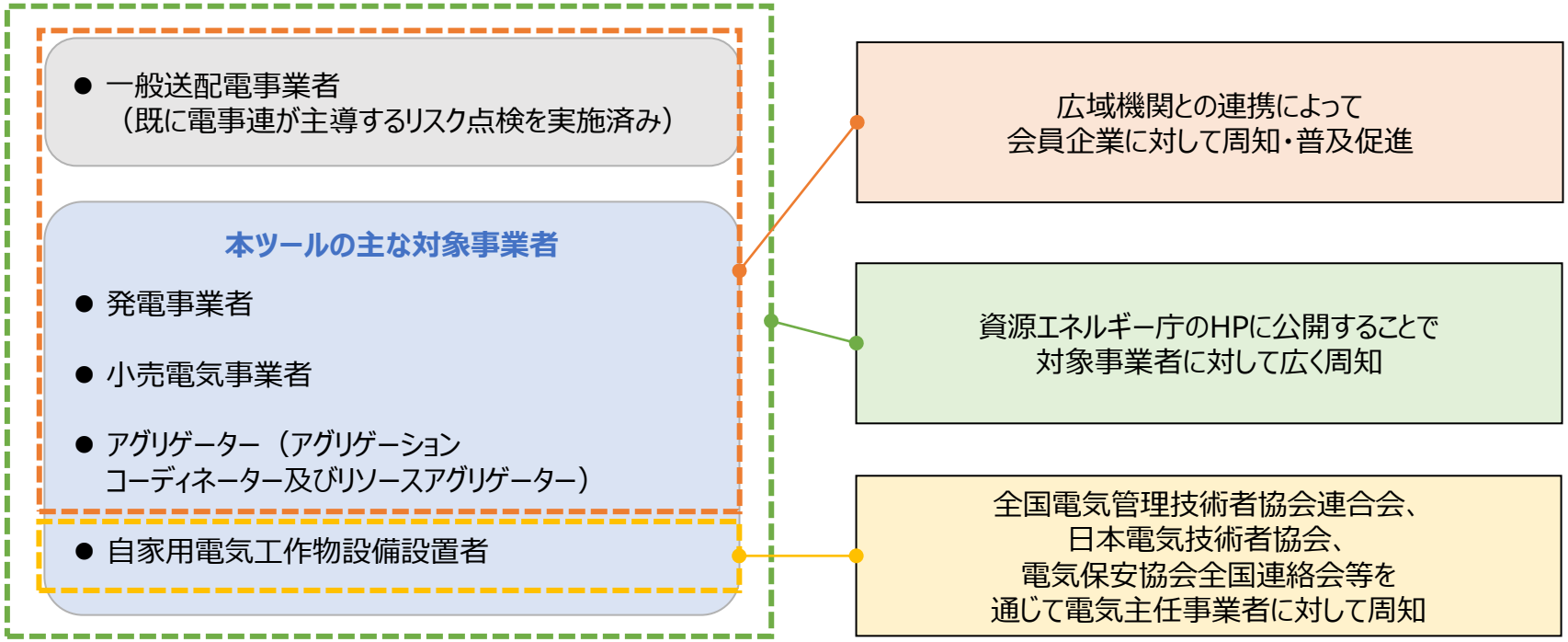
No	指摘事項	修正対応
1	サブカテゴリー「DE.AE-4」における「イベント」を具体的にイメージすることが難しい。	「イベント」を「セキュリティ事象」という用語に変更し、意味を明確化した。
2	サブカテゴリー「RS.RP-1」における「対応計画」が何を具体的に示しているか分からない。	「対応計画」を「インシデント対応計画」という用語に変更し、意味を明確化した。また、ガイドにおいても「インシデント対応計画」を用語集に追加した。
3	サブカテゴリー「ID.AM」全体の達成基準が、運用実態と制度構築に分かれているため、分割した別の設問に分けるとより分かりやすい。	達成基準はNIST-CSFに基づいて策定しているため、現状の記載にとどめる。本リスク点検ツールの評価基準では、事実的な運用を重要視し、運用制度の構築は追加ステップとして位置づけているところ、この方針について、ガイドやツールの使い方にも記載した。
4	可視化結果で評価が０になる際に、「活用区分」の選択により該当するチェック項目がない場合と該当項目の対策が実施できていない場合の区別がつかない。	「活用区分」の選択により該当項目がない場合は、可視化結果シートでグレーアウトされるよう修正した。
5	事業区分・規模に応じて、現状より項目を絞り込んでいただきたい。	ツールを任意活用する際は、事業者が必要だと思われる項目のみで評価することも可能である。参考としてサイバーセキュリティ経営ガイドラインのみに対応した項目のみで評価できることをガイドに記載した。
6	設問の達席基準に対して事業区分ごとに推奨されるレベルを示していただきたい。	広域機関の取組（後述）では、平均2点以上にすることを会員企業に推奨しており、参考値として本リスク点検ツールでも記載した。

１．リスク点検ツールの正式公開に向けた取組

2.　リスク点検ツールの普及展開・位置づけについて

任意ツールとしての周知・普及促進の方策

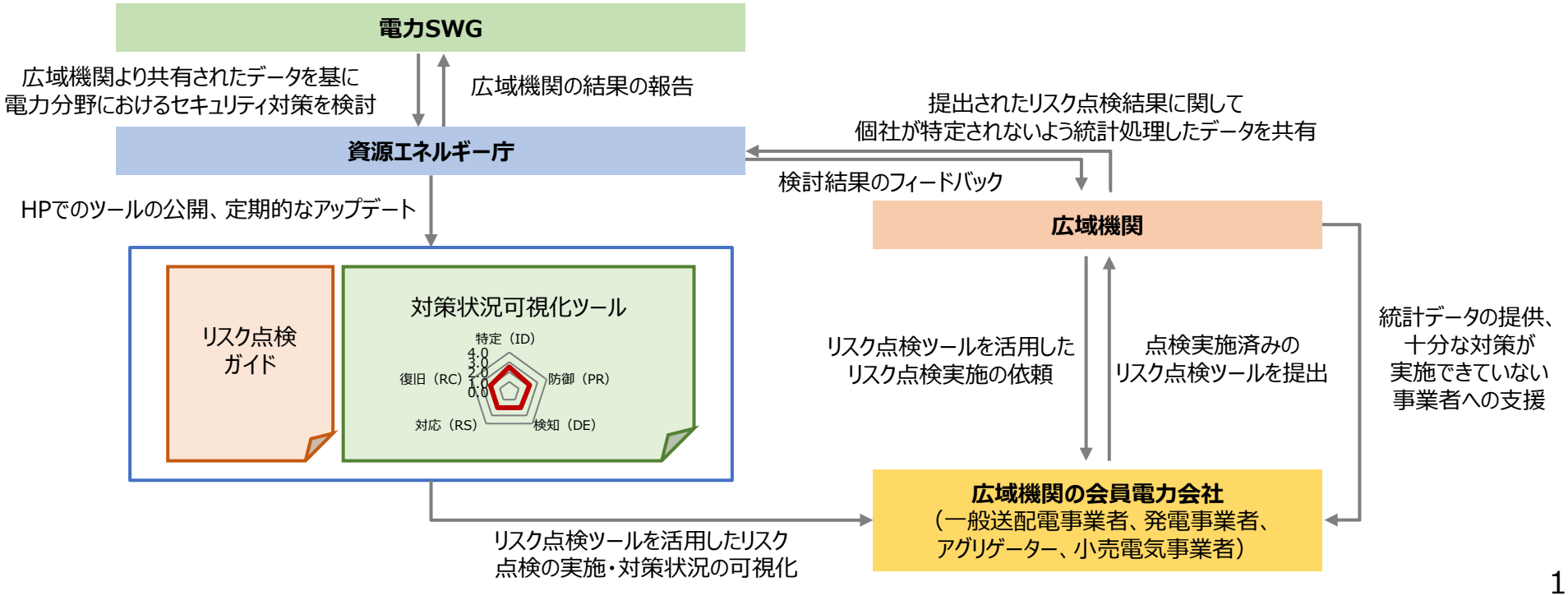
- 正式公開後には、任意ツールとしての周知・普及促進を予定している。
- リスク点検ツールの対象事業者のうち、**発電事業者、小売電気事業者、特定卸供給事業者については、登録・届出の際に、電力広域的運営推進機関（OCCTO）への会員登録が必須**である。そのため、**広域機関との取組の連携によって、これらの事業者に対しては、広く普及促進される**ことが想定される。
- 自家用電気工作物設備設置者に対しては、**必要資格である電気主任技術者の保持者を管理している全国電気管理技術者協会連合会（全技連）**、**電気主任技術者を主体とした日本電気技術者協会**、**保安協会を取りまとめている電気保安協会全国連絡会等**を通じて周知を行うことが効果的である。



広域機関の自己診断票との連携

- 昨年度のSWGで御報告のとおり、**広域機関の自己診断票を今回のリスク点検ツールと統合する予定**である。
- 資源エネルギー庁HPにてリスク点検ツールを公開後、広域機関では、**公開されたホームページを参照する形式でリスク点検の実施を会員企業に依頼**する。**会員企業は、エネ庁HPから公開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**する。
- 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く**。今後、**電力SWGにおいてはリスク点検ツールに対する取組状況や点検結果等も踏まえ、電力分野におけるセキュリティ対策のあり方を検討していく**。

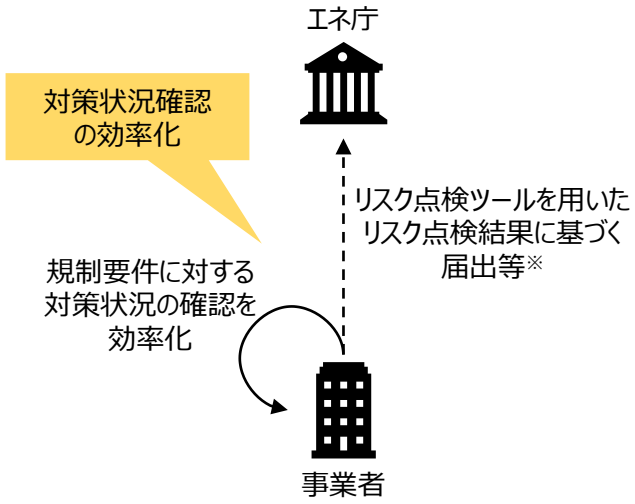
リスク点検ツールの広域機関との連携スキーム



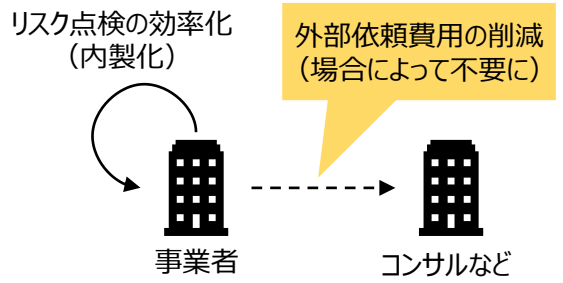
リスク点検ツール活用が事業者に与えるメリット

- リスク点検ツールの活用が事業者に与えるメリットとして、**合理的なリスク点検によるリスク可視化効果**のほか、規制においてセキュリティ対策が要求されている事業者においては、**規制要件に対する確認の効率化（①）**が想定されるほか、規制有無に関わらず**リスク点検に対するコスト低減効果（②）**が得られる。
- また、**第三者（外部委託事業者や保険会社など）に対するセキュリティ対策状況の説明（③）**に関しても活用可能であることも想定される。
- それぞれのメリットを事業者が享受できるよう、ツールの普及展開・位置づけを検討する必要がある。

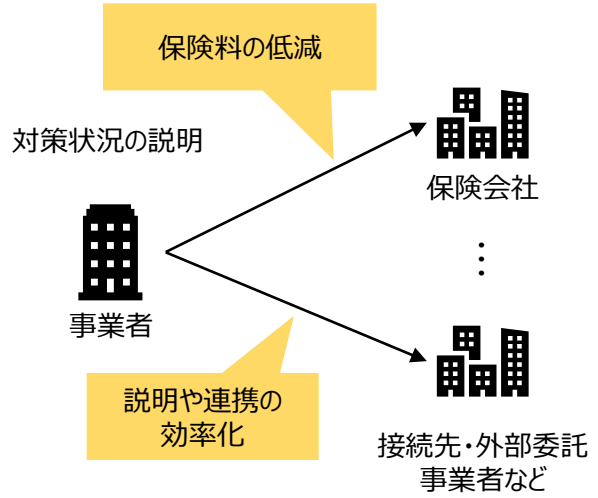
メリット①
規制要件に対する
対策状況確認の効率化



メリット②
リスク点検作業の低コスト化



メリット③
第三者に対するセキュリティ
対策状況説明の効率化



※ 特定卸供給事業者の届出に当たって必要な「サイバーセキュリティ確保実施内容一覧」の記入に当たってのリスク点検ツールの活用等

リスク点検ツールの位置づけに関するご意見

- 委員に対する事前の意見交換では、リスク点検ツールの位置づけについて、段階的な要求レベルの向上、事業区分・規模による位置づけ、支援・インセンティブに関する意見等が挙げられた。
- 多くの委員より、**段階的な要求レベルの向上の必要性について意見**をいただいた一方で、**全ての事業者に求めるのではなく、事業区分や規模に応じて検討する必要性も確認**された。特に、中小事業者に対するインセンティブや支援策を検討する必要性が示唆された。

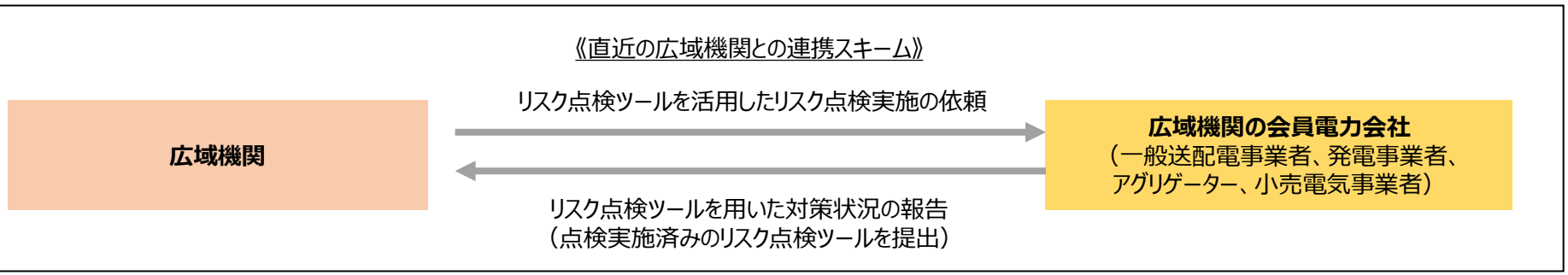
カテゴリ	意見
段階的な要求レベルの向上について	• 任意活用の位置づけから始めて、徐々に要求レベルを高めていく方針は良い。 • 段階的に要求レベルを高めるべきであり、プランをあらかじめ周知すべきである。 • 浸透状況を確認の上で、要求レベルを高めることが必要である。 • ツールの利用率などによって浸透状況を定期的に確認し、状況に応じて要求レベルを高めるのはどうか。
事業区分・規模による位置づけについて	• 規模の小さい自家用電気工作物設備設置者には周知やコスト負担に対して援助するなどが必要である。 • アグリゲーター等の他者にセキュリティ上の脅威を及ぼしうる事業者に対しては、リスクの自己点検を義務付けるべきである。その点検において、今回のツールを活用できる形でも良い。
支援・インセンティブについて	• インセンティブがないと特に中小に普及させることは難しい。 • 義務化するなら目的を明確化にしていただきたい。 • 利用に伴う管理コストを電気事業者に負担させないということもインセンティブになる。 • セキュリティ対策の能力がない事業者の能力を引き上げるための取り組みや、本ツールを利用しやすい環境をアウトソースできるような仕組みを作ることもインセンティブとなる。 • 経済的インセンティブの優先度は低く、電気事業者の外部経済部分を負担していくべき。
その他	• 経済安全保障推進法が施行されたが、この法律とリスク点検ツールの関連性を議論すべきではないか。 • 参照元ガイドラインのアップデートに合わせるためにも、点検ツールの定期的なアップデートが必要となる。 • 点検ツールの利用に関して、教育プログラムを用意する必要がある。 • 評価側のスキル向上に向けた取組も必要となる。教育や啓発に力を注いだほうが良い。特に中小企業に対する支援が重要となる。 • 自家用電気工作物に関する周知に関しては、保安業者を束ねている団体と連携できると良い。 • 各社が自ら点検を行うことに意義があり、結果を横並び比較するような取組は望ましくない。

意見交換を踏まえたリスク点検ツールの位置づけ

- 電気事業者の多くは広域機関の会員となるところ、リスク点検ツールの浸透・活用にあたっては、広域機関と連携した取組が効果的である。
- **広域機関と連携し、ツールの浸透状況やツールに基づくリスク状況を定期的に確認しつつ、当該状況を踏まえ、より踏み込んだ要求レベルの設定や支援策等の検討を行う**。

広域機関と連携したツールの位置付けに関する検討方針

《直近の広域機関との連携スキーム》



リスク点検ツールの浸透状況の定期的な確認

提出されたリスク点検結果の分析による電力分野全体のリスク状況の把握

浸透状況・リスク状況を踏まえたリスク点検ツールの位置付けの検討
（特定区分に対する要求レベルの向上、特定区分に対する支援 等）

御意見をいただきたい事項

- 試行利用の結果に基づき、リスク点検ツールを修正し、最終版のリスク点検ツール（資料7-2・資料7-3）を作成した。**修正したリスク点検ツールについて、本日の御議論を反映した上で、正式公開することとしてはどうか**。
- また、リスク点検ツールと広域機関との取組の連携について確認し、来年度から連携できるよう調整した。
- 委員への事前意見交換では、電力業界全体でリスク点検ツールの効果を高めるために、段階的な要求レベルの向上の必要性について意見をいただいた一方で、全ての事業者に求めるのではなく、事業区分や規模に応じて検討する必要性も確認された。
- 段階的に要求レベルを向上させるうえでは、**電気事業者の多くが会員である広域機関の取組との連携が重要**である。広域機関の取組と連携しつつ、ツールの普及状況やリスク点検状況等を確認した上で、**必要に応じて要求レベルを高めていくことが現実的**である。
- **広域機関の取組と連携し、要求レベルの向上を検討する上で、事業者のどのような状況を考慮するべきか。**
（例：事業規模、事業区分、電力システムとの接続の有無、リスク点検状況など）
- また、**リスク点検ツールの要求レベルの向上にあたって、どのようなインセンティブ・支援を検討していくべきか。**
（例：保険会社と連携してリスク点検ツール活用によるサイバー保険料の低減等のインセンティブの検討、リスク点検を外部委託する際の活用の促進など）