経済産業省

資料７

公表用

リスク点検ツールに基づく
自己診断結果の分析について

2025年2月4日

資源エネルギー庁　電力産業・市場室

リスク点検ツールに基づく自己診断結果の分析について

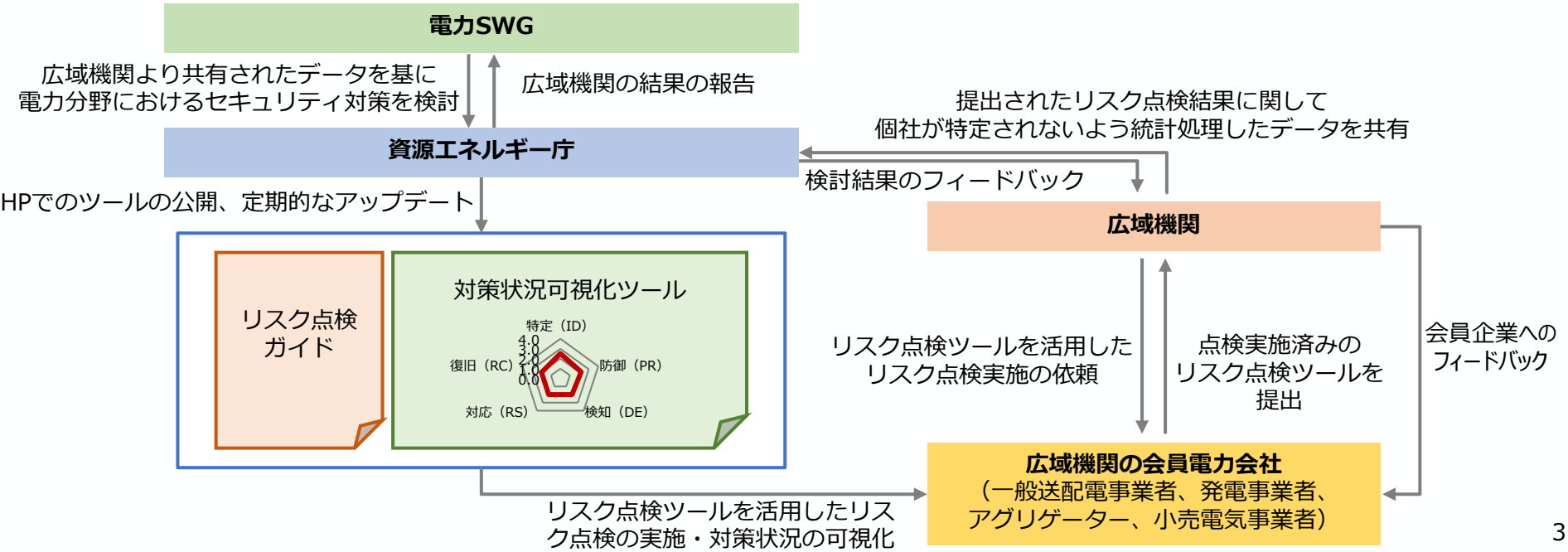
- 昨年度、電気事業者を主な対象として、過大なコストをかけずに簡易的にリスク点検ができるよう、「電力システムにおけるサイバーセキュリティリスク点検ガイド」及び「電力システムにおけるサイバーセキュリティ対策状況可視化ツール（リスク点検ツール）」を開発し、2024年3月に公表した。
- 今年度より、電力広域的運営推進機関（OCCTO）が実施する電気事業者のセキュリティ自己診断の取組において、リスク点検ツールを活用した取組を実施している。
- 本取組を実施するにあたり、リスク点検ツールの使い方に関する説明会を開催した。
- 本日は、説明会の実施概要と、広域機関が実施した電気事業者の自己診断結果の分析結果を示す。分析結果を踏まえ、今後必要なセキュリティ施策のあり方について御議論いただきたい。

（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

- 今年度より、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している。
- 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いた。

リスク点検ツールの広域機関との連携スキーム



（参考）広域機関の取組との連携スケジュール

第17回電力SWG
資料を一部修正

- 2024年11月より、広域機関による今年度のセキュリティ自己診断の取組を実施した。
- 今年度から、リスク点検ツールを活用した取組に変更したところ、リスク点検ツールの普及及び自己診断の対応率増加を目的に、リスク点検ツールの使い方に関する説明会を開催した。

広域機関の会員企業向けのリスク点検ツールの説明会

- 広域機関の会員企業向けに、リスク点検ツールの使い方に関する説明会を2回開催した。
- 説明会では、**説明会の目的・概要、広域機関の自己診断の必要性、リスク点検ツールの概要、本取組におけるリスク点検ツールの使い方について具体的に解説**した。
- 説明会はオンラインで実施し、各回100名以上が参加した。

説明会の概要

説明会の目的
自己診断の取組の目的の紹介と今年度から連携するリスク点検ツールの利用方法の説明

開催日時
第1回：2024年11月6日（水）　13:00-14:00（114名参加）
第2回：2024年11月14日（木）　11:00-12:00（156名参加）

開催方式
オンライン

案内方式
広域機関より会員企業へ案内を発出（任意での参加）

アジェンダ
1. 説明会の目的・概要
2. 広域機関の自己診断の概要
3. リスク点検ツールの概要
4. 本取組におけるリスク点検ツールの使い方
5. 質疑応答

（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
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