資料２－３

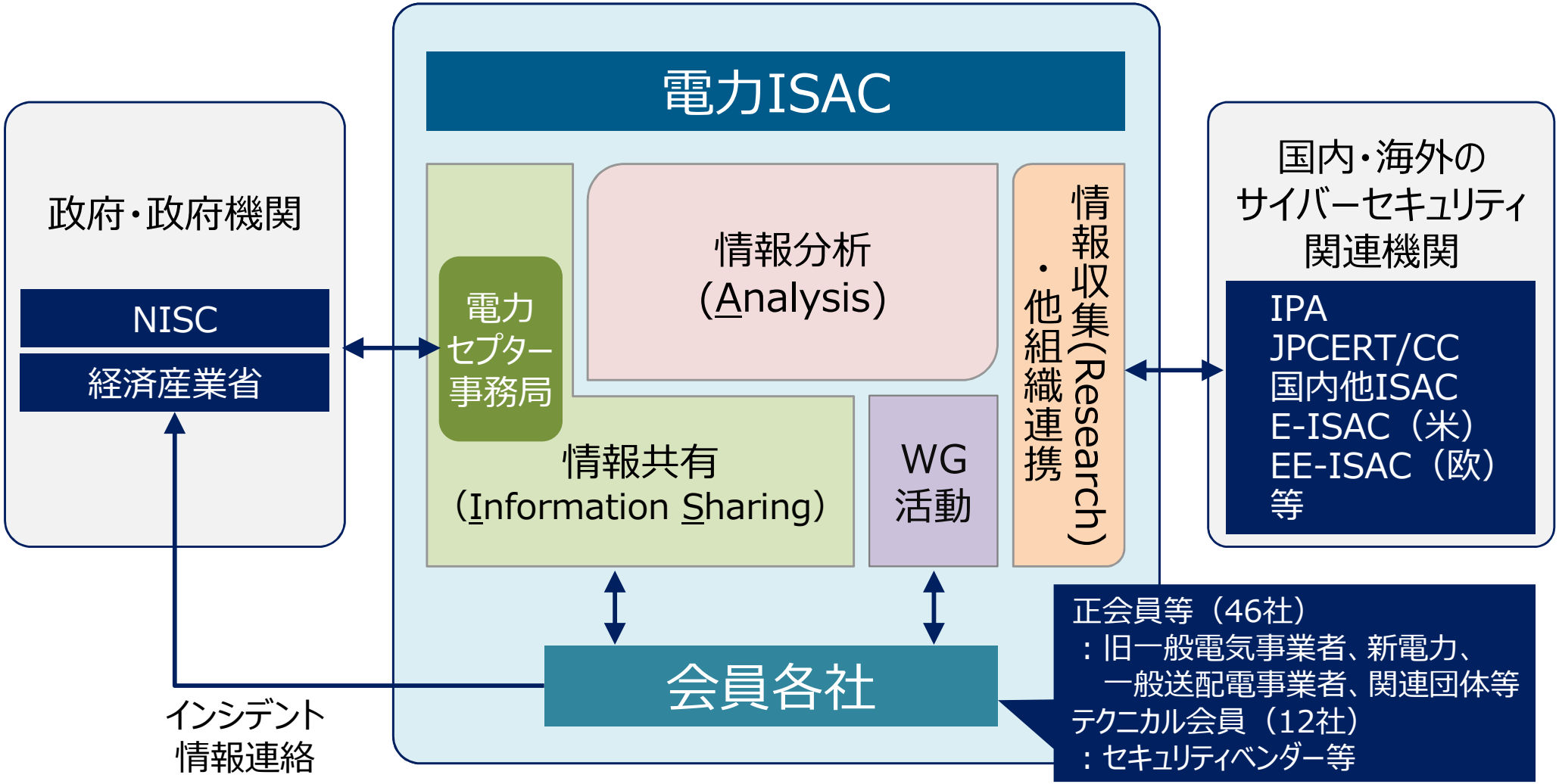
電力ISACの事業概要、および「議論の整理」の受け止めについて

2024年9月2日
電力ISAC

JE-ISAC Japan Electricity Information Sharing and Analysis Center

電力ISACについて

- 会員間で信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換・分析、電気の安定供給及び電気事業に係る情報の安全性や業務の継続性の確保に資する



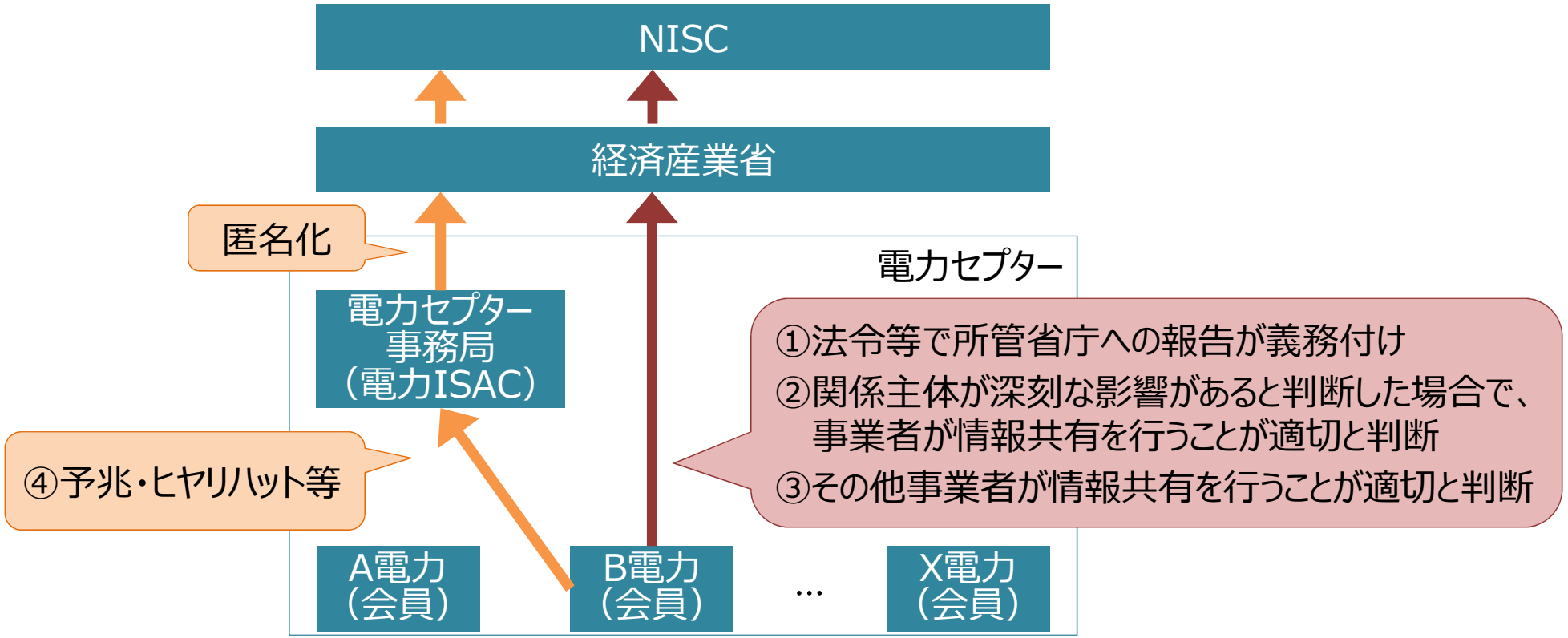
電力ISACについて：事業概要

- 諸機関や他ISACからの情報収集、情報分析を行い、会員各社との情報共有を実施
- WG活動等を通じて、会員間での意見交換やセキュリティ確保への対応力向上を図る

分類	項目	取り組み
情報収集	諸機関の提供情報の収集	NISC、IPA、JPCERT/CC等から提供される情報を収集
	他組織連携	国内の他分野ISAC、米・欧電力ISAC等との情報連携により、サイバー脅威に関する情報収集および関係構築
情報分析	OSINT	国内外のインシデント事例、政策動向等の公開情報をもとに、電力事業者向けの示唆を収得
	分析レポート発行	サイバー脅威動向・制度動向などについて電力事業者影響の観点から分析したレポートを発行
情報共有	収集・分析情報の発信	収集・分析した情報を会員向けに発信
	会員からのインシデント情報、予兆・ヒヤリハット情報の発信	行動計画に基づく所管省庁向けの情報連絡の同報受信等から、必要に応じて匿名化の上で会員へ共有
	テクニカル会員からの発信	ソフトウェア脆弱性等の情報を会員へ共有
	総会カンファレンス開催	政府機関・関連機関のご講演、テクニカル会員のブース展示等
WG活動他	ワーキンググループ活動	会員が主体となり、取組状況の共有や、課題解決を行う
	技術勉強会・ハンズオン演習	テクニカル会員が講師となり、会員の対応力向上のために開催

電力ISACについて：行動計画に基づく情報連絡（現状）

- 電力は、電気関係報告規則に定める供給支障についての報告義務の他、サイバー攻撃に起因するおそれのある事故等、社会的影響を及ぼす可能性のあるインシデントについて、行動計画に基づき事業者から所管省庁へ情報連絡
- 予兆・ヒヤリハットや上記以外のインシデントについて、必要に応じて匿名化を施したうえ、電力セプター事務局より所管省庁へ情報連絡



議論の整理への受け止め：政府の情報提供・対処を支える制度

- 国民生活の基盤をなす経済活動や社会の安定を守るため、高度な侵入・潜伏能力を持つサイバー攻撃への対策の有効性確保に向けた、官民連携強化の必要性を理解
- 電力分野含め、行動計画に定める重要インフラ事業者は社会基盤を担う事業者であり、攻撃者による侵入・潜伏のターゲットともなり得るため、実効性のある対策が必要

インシデント報告の義務化の対象

✓ インシデント報告の義務化の対象について、事業者での円滑な対応が期待されることから、行動計画に示される重要インフラサービス障害の報告に係る法令・ガイドライン等、**既存の根拠法令等（電力分野では電気関係報告規則）における報告義務の対象と整合**を取っていただきたい

効果的な情報共有の方法・タイミング

✓ サイバー攻撃に起因する供給支障等発生時、**電気事故**報告と**サイバー攻撃**に関する報告義務がそれぞれ生じる。新たなサイバー対応組織において、**サイバー攻撃に関する報告窓口を一元化**いただき、政府内での省庁間の密な連携をお願いしたい

✓ 供給支障等の事故の**初報**連絡時、**システム不具合**によるかの**切り分けが未済**の場合があるため、電気事故報告とサイバー攻撃報告窓口への**報告タイミング**は**各々に即した**ものとしていただきたい

議論の整理への受け止め：ソフトウェア等の脆弱性対応

- 近年のサイバー攻撃において、重要インフラ事業者のOTシステムに至る侵入手段として、ゼロデイ脆弱性が積極活用されている状況より、ソフトウェア等について迅速なリスク情報の提供を受けることは、サイバー攻撃への対応力の向上に有益

脆弱性情報の迅速な共有

- ✓ ソフトウェアベンダー側の**脆弱性公表のスピード感**を高める施策検討・対応への注力が有効と思料
- ✓ 脆弱性の情報と共に、**侵害有無の調査方法**や**緩和策**などの情報を併せて提供いただくことにより、各分野の重要インフラ事業者が迅速に有効な対策を打てるものと思料

議論の整理への受け止め：高度な攻撃に対する支援・情報提供

- 攻撃者の侵入検知のための脅威ハンティング実施にあたり、政府から提供いただくインテリジェンス情報および攻撃手法に関する情報は有益
- 諸機関の提供情報をISACが収集して会員各社へ展開する現状に対し、官民協議会におけるワンボイスでの情報提供は、事業者の迅速な対応に資すると思料

効果的な情報共有の方法

- ✓ 重要インフラ事業者に限らず、ISAC会員や製造ベンダー、セキュリティベンダー等、重要インフラに関連する**ステークホルダーを含めた**官民の協議会とすることが望ましいと思料
- ✓ 迅速な情報展開が必要であると考えられることから、各事業者へ**直接情報提供**いただきたい
- ✓ **国の情報共有の仕組みの中**で、情報の区分毎に**アクセス権限**を定めセキュアに提供いただきたい

セキュリティクリアランスの取得

- ✓ 適合事業者認定や従業員等が適正評価を受けるにあたり、**情報管理体制**の構築、**プライバシー**保護および労働法令との整合等、慎重な検討が必要
- ✓ セキュリティクリアランス必須の情報提供がなされる場合、**対象情報を厳選**いただくと共に、セキュリティクリアランス取得に係る**ガイドラインや解説集**の提供等、手厚いフォローをお願いしたい

議論の整理への受け止め：人材の育成・確保、中小企業を含めた対策

- 電力ISAC会員各社においても、サイバーセキュリティ人材確保に苦慮する状況にあり、サイバーセキュリティに係る仕事が魅力あるキャリアとして認知されるべく、取組を継続中
- 中小企業を含めた重要インフラに係るサイバーセキュリティ対策の強化も重要な課題

サイバーセキュリティ人材の育成

✓ **OTシステム**はITに比べて**汎用性が低い技術**も利用しており、個社での育成は非効率であるため、OTも含め民間サイドが効果的に育成できるような**育成機関**や**コースの継続・新設**をお願いしたい

✓ **効率的に情報共有**を行うため、情報提供側においても**OTシステムの技術や運用**を考慮の上、現実的かつ効果的な対応をできる人材育成を継続してお願いしたい

中小企業を含めた対策強化

✓ 重要インフラ事業者における**委託先・再委託先等のセキュリティリスク**を考慮すると、中小企業においても大企業に遜色のない対策を求める必要があると思料

✓ **社会全体の強靭性**を高めるため、個社および委託元による対応に加え、中小企業における体制整備・費用・的確なアドバイス等のサポートについて、国大での支援をお願いしたい