一般社団法人 送配電網協議会
Transmission and Distribution Grid Council

公開用

説 明	資料5

第20回 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ＳＷＧ

送配電事業におけるサイバーセキュリティ対応の重要性と今後の対応について

2026年10月19日

一般社団法人送配電網協議会

本日のご説明内容

○ フロンティアAIの出現によりサイバー脅威は新たな段階に入っており、電力の安定供給を担う一般送配電事業者のサイバーセキュリティ対策の重要性はこれまで以上に高まっている。

○ 本資料では、**①送配電事業におけるサイバーセキュリティ対応の重要性（技術的観点）**、および**②託送料金制度（RC制度：レベニューキャップ制度）における投資の考え方**についてご説明する。

①

送配電事業におけるサイバーセキュリティ対応の重要性（技術的観点）
(1) フロンティアAIの出現によるサイバー脅威の変化
(2) 一般送配電事業者のセキュリティ対策の重要性
(3) 一般送配電事業者のサイバーセキュリティ強化の方向性
(4) 国からの要請との関係

②

託送料金制度（レベニューキャップ制度）における投資の考え方
(1) 託送料金とレベニューキャップ制度
(2) レベニューキャップ制度におけるサイバーセキュリティ対策の必要性評価
(3) レベニューキャップ制度におけるサイバーセキュリティ対策の制度上の扱い

フロンティアAIの出現によるサイバー脅威の変化

○ 脅威環境は構造的に変化しており、フロンティアAIが悪用された場合、サイバー攻撃のスピード・規模は劇的に増加するおそれがある。

○ 脆弱性の発見件数が増加し、発見から攻撃に悪用されるまでの期間も短縮される。このため、パッチ適用の頻度と迅速性の向上が求められ、防御側の負担は増大する。

○ **電力の安定供給を担う一般送配電事業者には、こうした脅威の変化への対応の必要性が高まっており、確実に対応していく必要がある**。

	これまで		フロンティアAI時代
脆弱性の発見	専門人材による探索が中心	→	AIにより大量の脆弱性が発見
攻撃のスピード・規模	人手に依存し、一定の時間を要する	→	攻撃のスピード・規模が劇的に増加
防御側の負担	計画的なパッチ適用で対応	→	パッチ適用の高頻度化・迅速化に伴う運用リソースの逼迫
防御の考え方	「境界型防御」が中心	→	従来の境界型防御に加え、侵入を前提とした「ゼロトラスト」を追加

出典：資源エネルギー庁ほか「フロンティアAIによる脅威変化を踏まえた電気事業者等の短期的な対応に係る要請」（令和8年7月8日）等をもとに作成

一般送配電事業者のセキュリティ対策の重要性

○ 送配電網は、**国民生活・経済活動を支える重要インフラであるため、サイバー攻撃によるシステム侵害により、電力の安定供給や事業運営に支障が発生するおそれ**がある。



送配電事業を支えるシステム

・電力系統の運用、送配電設備の監視・保全
・託送・計量・料金、設備の工事管理等に関する業務　等

→ **システムが停止すると、電力の安定供給や事業運営に支障が発生するおそれ**

フロンティアAIによる脅威の増大は、送配電事業を支えるシステム全体に及ぶ
・システム構成機器の脆弱性の大量顕在化
・外部との接続や保守・調達等を介したシステム侵害リスク 等

→ **システム全体のリスクを総合的に捉えた多層的な対策が必要**

一般送配電事業者のサイバーセキュリティ強化の方向性

○ 前頁までの脅威の変化と送配電事業を支えるシステムの特性から課題を整理し、以下の3つを柱とした**サイバーセキュリティ対策の抜本的高度化を推進**する。

○ サイバー攻撃と防御は終わりなき高度化競争であり、単発的な対応ではなく、**継続的な見直し・強化を前提とした基盤整備**と位置付ける。

1

課題 | 境界防御だけでは、侵入後の内部での攻撃・横展開を防ぎにくい

ゼロトラストの考え方に基づく対策の導入

「境界型防御」等の既存対策の徹底を前提としつつ、システムの安定稼働を維持しながら、内部においても全てのアクセスを信頼せず、あらゆる挙動を常に検証する「ゼロトラスト」の考え方を取り入れ、内部通信の制御・監視、不正検知、多要素認証、資産管理の高度化等を推進する。

2

課題 | 脆弱性の大量発見に、人手や古いシステムでは追随が難しい

フロンティアAIなどを活用した対策の高度化

フロンティアAI等を脆弱性管理や脅威の検知・対応に活用し、運用の高度化・効率化を推進する。また、多層防御・横展開防止、レガシーシステムの計画的な刷新、クラウドやAI利用に伴うリスクへの対策を強化する。

3

課題 | 侵入を完全には防げず、システム停止が事業運営に波及するおそれがある

事業継続・復旧力（サイバーレジリエンス）の強化

サイバー攻撃による侵入・被害発生を前提に、サイバーBCPの整備、隔離型リカバリ環境や、能動的なサービス停止・ネットワーク遮断の仕組み等を構築し、被害の極小化と早期復旧を図る。

国からの要請との関係

○ 令和8年7月8日付で国から電気事業者等に対し、フロンティアAIによる脅威変化を踏まえた短期的な対応が要請されており、前頁までの一般送配電事業者の取組みは、本要請とも方向性を同じくするもの。

○ 要請では、サイバーセキュリティを経営課題として扱い、ゼロトラストの考え方の導入、必要なリソース（予算・人員）の確保、レガシーシステムのアップグレード等が求められている。

◎：特に関連が強い柱　○：関連する柱

		P.5の3つの柱との対応		
		柱1	柱2	柱3
経営課題として扱う	経営トップのリーダーシップのもと、経営層が直接関与し必要なリソースを確保	3つの柱全体の推進基盤		
基本的な対策の徹底	侵入口の縮小、検知・監視、多要素認証、バックアップ確保	◎	○	○
ゼロトラストへの移行	従来対策に加え、マイクロセグメンテーション、内部システムの常時監視・検知等の追加	◎	○	
パッチ適用増加への備え	予算・人員の確保、リスクベースでの優先順位付け	○	◎	
パッチ以外の対策強化	多層防御・横展開防止、レガシーシステムのアップグレード計画と予算確保、障害・停止への備え、能動的サービス停止	○	◎	◎
AI活用に向けた準備	AI活用範囲・情報管理・脆弱性管理の社内ルール整備、人材確保・教育		◎	
業界内外の連携強化	電力ISAC等を通じ、他業界も含めた情報収集・共有による分野全体の強靭化	3つの柱全体の推進基盤		

出典：資源エネルギー庁ほか「フロンティアAIによる脅威変化を踏まえた電気事業者等の短期的な対応に係る要請」（令和8年7月8日）をもとに作成

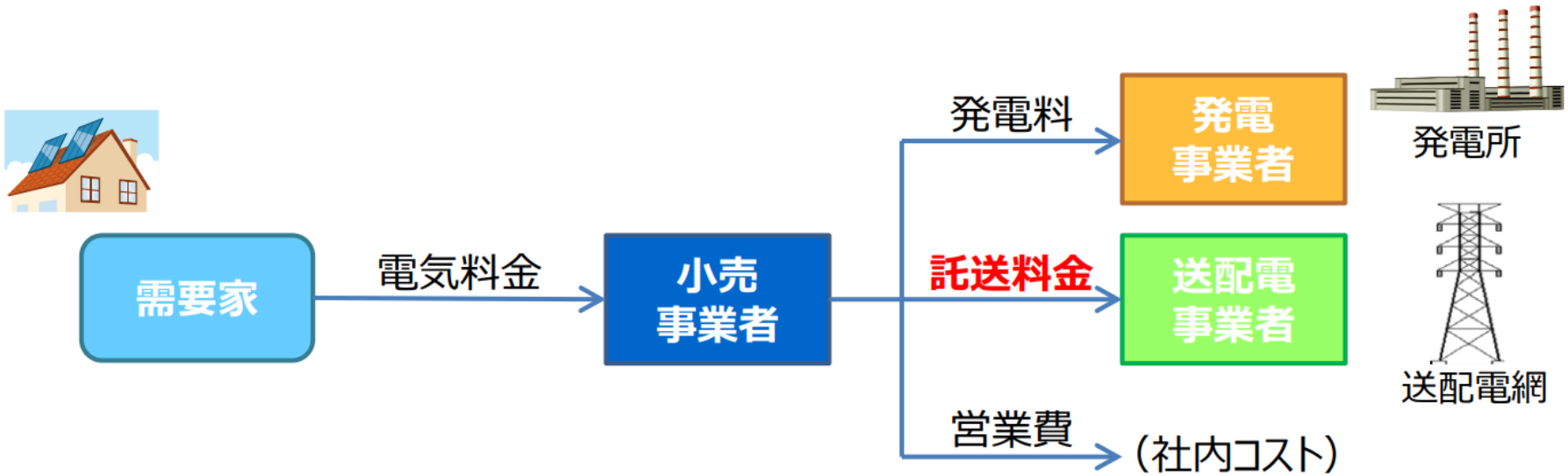
託送料金とレベニューキャップ制度

○ 一般送配電事業者は、**「電気を送る」ために必要な費用を「託送料金」**として回収し、送配電設備の維持・更新等の事業活動に充てている。

○ また、託送料金は、電気の安定供給に必要な費用を確保しつつ、利用者の負担にも配慮する必要があることから、経済産業大臣の認可を受けて設定する仕組みとなっており、その制度として**「レベニューキャップ制度」**が導入されている。

＜電気料金の構成と託送料金＞

資源エネルギー庁 HPより引用
（一部加工）



電気料金	
	発電料
	託送料金
	営業費
	利潤

←家庭向け電気料金の30～40%程度

（送配電部門の人件費や送配電設備に係る修繕費、減価償却費など）

レベニューキャップ制度の目的

○ **レベニューキャップ制度は、電力の安定供給やカーボンニュートラルの実現等に必要な投資費用を確保するとともに、事業者の効率化を促す仕組みとして、2023年度より導入**されている。

（必要な投資費用の確保）

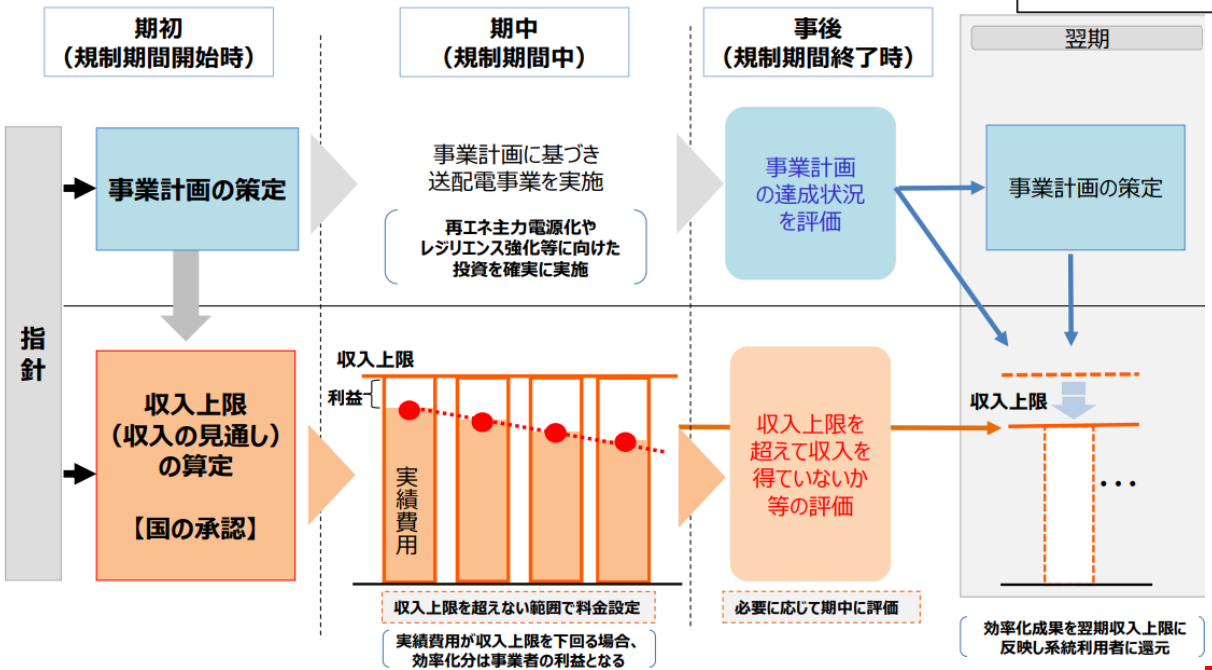
- ✓ 一般送配電事業者は、国の指針に基づき**5年間の規制期間の事業計画を策定し、**その間必要となる費用の見積等を申請し、**国による審査を経て、託送料金の収入上限（レベニューキャップ）を決定**
- ✓ 予見困難な需要や費用の増減は、規制期間中または翌規制期間に調整を実施

（事業者の効率化インセンティブ）

- ✓ 前規制期間における**効率化の成果を利用者への還元と事業者の効率化インセンティブに配分することで、託送料金の低廉化と事業者の効率化の促進を両立する。**

＜レベニューキャップ制度の全体像＞

託送料金制度（レベニューキャップ制度）
中間とりまとめ



レベニューキャップ制度におけるサイバーセキュリティ対策の必要性評価

○ **サイバーセキュリティ投資**は、収益創出を目的とするものではなく、重大事故の未然防止および事業継続性の確保という**社会的責務を支えるものであり、「必要投資」と認識**

○ その性質上、B/Cによる定量評価だけでは測りきれないため、**安定供給・事業継続等の観点から必要性を総合的に評価（定性評価）することが適当**である。

一般的な設備投資

・便益(B)の定量化が可能
・B/Cにより投資判断

サイバーセキュリティ投資

- 被害の未然防止・低減が目的のため、効果が顕在化しにくい
- 攻撃の手段や頻度は攻撃者に依存するため、被害額・発生確率の見積りが困難
- 攻撃手段は日々高度化するため、状況変化に応じた継続的な投資が必要

評価方法（例）：定性的な観点による総合評価

安定供給・サービス水準の維持
攻撃が高度化・増加する状況下においても、電力供給・お客さまサービスへの重大な影響を抑制できるか。

インシデント対応力の向上
攻撃検知から初動・封じ込め・復旧までの体制を整備し、対応の練度を高められるか。

事業継続への影響抑制
攻撃時の業務停止・縮小による事業への影響・負担を低減できるか。

脅威変化への追随
セキュリティ対策の点検・評価を実施し、対策の継続的な見直し・強化を図れるか。

レベニューキャップ制度におけるサイバーセキュリティ対策の制度上の扱い

○ サイバーセキュリティ対策は、脅威・技術の変化に応じて継続的な強化が必要であることから、レベニューキャップ申請においても、**期初の適切な計上に加え、期中の追加・変更や事後の確認・調整を柔軟に行える制度上の取扱いが必要**である。

○ また、既に実施している取組みについても、その実施状況・内容等を確認し、必要に応じて適切に事後調整することが必要である。

項 目	考え方
期初	P.9で示した考え方に基づき、**必要なサイバーセキュリティ投資を適切に織り込む**
期中	フロンティアAI等による新たな脅威や技術の進展により、**期初には想定していなかった対応が必要となる場合にも、投資の追加・変更が可能な仕組み**
事後	実施した投資について、**実施状況や取組内容等を確認したうえで、必要に応じて次期以降の取扱いに反映・調整する仕組み**
継続的な対応	レガシー刷新等、**複数の規制期間にわたり継続的に取り組む必要がある投資についても、脅威・技術の変化を踏まえ、継続的に対応できる仕組み**

期初：必要な投資の適切な織込み → **期中：環境変化に応じ柔軟に追加・変更** → **事後：実施状況を確認し必要に応じて調整**

脅威・技術の変化が続く中でも、安定供給・事業継続に必要なセキュリティ水準を維持・向上できるレベニューキャップ制度とすることが重要

まとめ

○ フロンティアAIの出現により脅威環境が構造的に変化する中、**送配電網のサイバーセキュリティ対策は、電力の安定供給および送配電事業の運営に直結する最重要課題の一つ**である。

○ 一般送配電事業者は、業界ガイドラインに沿った対応に加え、**送配電事業を支えるシステム全体のリスクを総合的に捉えた更なる対策強化に確実に取り組む**。

1

システム全体を総合的に捉えた継続的な対策強化

業界基準に基づく既存対策を維持・強化しつつ、送配電事業を支えるシステム全体において、ゼロトラストの考え方を取り入れた多層的な対策と、事業継続・復旧力（サイバーレジリエンス）の強化を継続的に進める。

2

レガシーシステムの計画的な刷新

脅威・技術の変化に継続的に対応できるよう、レガシーシステムのアップグレードについて、複数の規制期間にわたる計画的な投資により着実に進める。

3

「必要投資」としてレベニューキャップ申請に計上

一般送配電事業者が連携のうえ、安定供給・事業継続等の観点から必要性を総合的に評価（定性評価）し、必要な投資を適切に計上する。あわせて、期中の追加・変更や複数の規制期間にわたる継続的な取組みにも対応できる制度上の取扱いが重要である。