経済産業省

資料３

電力分野のサイバーセキュリティ対策に関する直近の動向

2026年10月19日

資源エネルギー庁

目次

１．電力分野のサイバーセキュリティ対策におけるJC-STAR制度の活用について　2

２．高性能AI等の技術革新に対する対応について　16

３．サイバー対処能力強化法及び整備法の施行について　28

１．電力分野のサイバーセキュリティ対策における JC-STAR制度の活用について

分散型電源（太陽光、蓄電池、風力、燃料電池）の系統接続におけるJC-STAR★１ラベル取得の要件化（2027年4月～）

- 近年、太陽光発電設備や蓄電池等の分散型電源の導入と電力系統への接続が急速に進む中、**分散型電源に対するサイバーセキュリティ上のリスクが指摘**されている。海外における分散型電源に対するサイバー攻撃の事例に加え、国内においても、太陽光発電の監視装置に内在する脆弱性が悪用され、サイバー攻撃の踏み台にされる事案が発生している。

- 現状、「電気設備に関する技術基準を定める省令」において、50kW以上の事業用電気工作物においてはサイバーセキュリティの確保が義務付けられているが、**50kW未満の小規模太陽光発電設備（一般用及び小規模事業用）については、サイバーセキュリティの確保に特化した明確な技術基準の規定までは存在しない**。

- こうした状況を踏まえ、電力の安定供給を確保する観点から、送配電網に接続する**太陽光発電や蓄電池等の分散型電源のサイバーセキュリティ対策**として、一般送配電事業者の系統連系に関するルールを改定し、**2027年４月以降に新たに系統接続するPCSやEMS等のIP通信機能を有する機器に対して**、最低限確保すべきサイバーセキュリティ水準を求める**JC-STAR★1の取得を要件化**することとした。

JC-STAR★1要件化に関する議論の経緯

- 系統WGでの審議を踏まえて電力広域的運営推進機関（以下、広域機関）に設置されたグリッドコード検討会において、本SWGでの議論を踏まえ、太陽光・蓄電池等の分散型電源におけるJC-STAR★1を活用したサイバーセキュリティ対策について検討を行ってきた。

電力SWG	系統WG・グリッドコード検討会
	2019年3月　第20回系統WGにて、**グリッドコード検討・整備を広域機関にて行う**こととした
	2020年9月　グリッドコード検討会を広域機関に開設
2024年10月　第17回電力SWGにて、**同年5月の太陽光向け遠隔監視装置におけるインシデント発生**を受け、**太陽光におけるサイバーセキュリティ対策の必要性**を議論	
2025年2月　第18回電力SWGにて、**太陽光等の分散型電源におけるサイバーセキュリティ対策の必要性**を議論	
	2025年6月　第19回グリッドコード検討会にて分散型電源におけるサイバーセキュリティ対策の要件化を**議論開始**
	2025年12月　第20回グリッドコード検討会にて、**太陽光・蓄電池**における**JC-STAR★1要件化**の方針を決定
2026年2月　第19回電力SWGにて、**グリッドコード検討会での議論状況**（太陽光・蓄電池におけるJC-STAR★1要件化の方針決定）を**報告。風力や燃料電池**等での要件化・**JC-STAR★２以上の基準整備の必要性**についても検討	
	2026年3月　第21回グリッドコード検討会にて、**風力・燃料電池**における**JC-STAR★1要件化**の方針を決定
	2026年10月　第13回次世代系統WG

要件化に向けた準備状況

- 今回の要件化を来年４月から実施するための準備として、**太陽光発電や蓄電池等の設置・運転に関わる事業者や機器メーカーへの周知・広報**、**FAQの作成**などを実施。

準備のための取組

- 事業者からの**系統接続の申込みプロセス等に関する問合せや相談**に対応し、例えば下記の論点について、**資源エネルギー庁ホームページにおいてFAQを公開**。
  - 新たな要件が適用されるタイミング
  - IP通信機能を持たない機器は対象外であること
  - 対象設備の増設やFIP転／卒FITの場合の取扱い
  - 機器故障時の機器交換の際の要件適用　等
- IPAの確認を受けた**JC-STAR★1取得製品は順調に増加**。各機器メーカーにおいて**ラベル取得に向けた開発・申請が進展している**ことをヒアリングで確認。

要件化を盛り込んだ**「電力品質確保に係る系統連系技術要件ガイドライン」の改定案**の**パブリックコメントを実施中**。

対象電源、適用開始時期及び適用範囲

- 分散型電源は多数のIP通信機器により構成され、ゲートウェイや遠隔監視装置以外の通信機器について、**インターネット等に直接露出していない場合であっても、IP通信機能を有する以上、外部からの侵入等のリスクが存在**。このため、**外部通信の結節点となるゲートウェイだけでなく、IP通信機能を有する個々の構成機器も対象**としている。

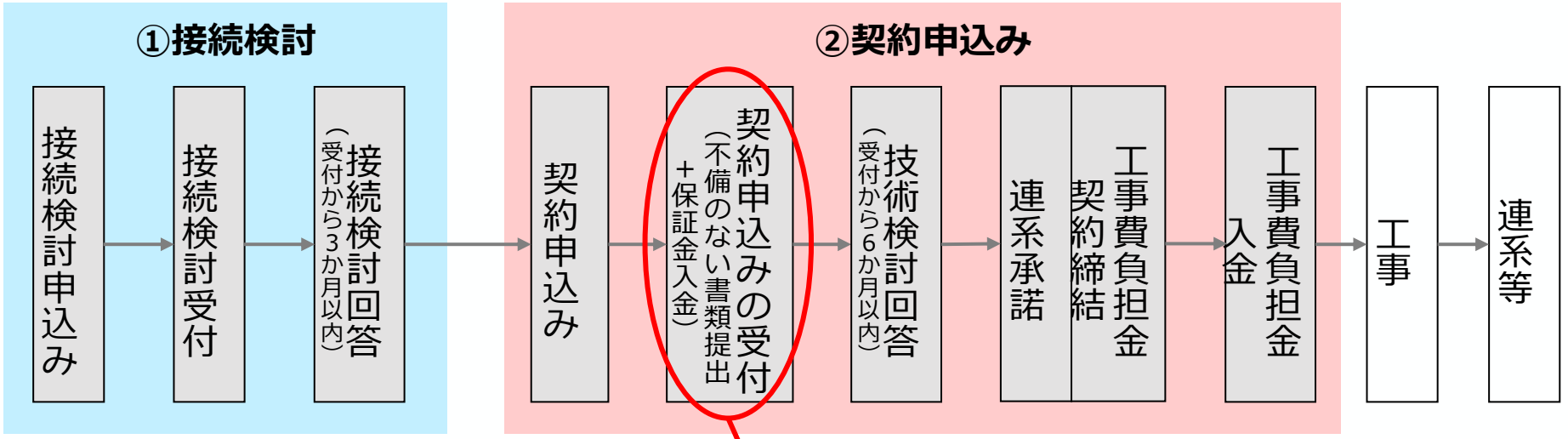
要件化の対象となる電源種、適用開始時期、適用範囲

電源種	適用開始時期	適用範囲
太陽光発電 蓄電池	**特高・高圧：2027年4月 低圧：2027年10月**	**ゲートウェイ**やその他の**IP通信機能を有する機器（PCS、BMS、EMS等の出力制御装置、遠隔監視装置）、ゲートウェイ等を介さずに主要な構成製品（制御システムやモジュール）と通信上接続しているIoT機器。**
燃料電池※1	**2028年4月**※2	**ゲートウェイ**やその他の**IP通信機能を有する機器、ゲートウェイ等を介さずに主要な構成製品と通信上接続しているIoT機器。**
風力発電※3	**2027年4月**	**ゲートウェイのファイアウォール（又はこれと同等の機能を有する機器）。**

※1：燃料電池のうち、逆変換装置を用いる形式が対象。ガスエンジン等に関しては適用範囲について現在検討中。
※2：必要に応じて経過措置の導入を検討。
※3：対象範囲の拡大やその適用開始時期について現在検討中。

新たな要件が適用されるタイミング

- 送配電等業務指針に基づき、2027年4月に変更される系統連系技術要件は、施行期日（2027年4月1日）以降に系統アクセスにおける**契約申込みを一般送配電事業者が受け付けた案件に適用**される。
- 要件化のタイミング前に契約申込みの受付が完了している案件について、**JC-STAR★1を未取得の機器を使用**していたとしても、**本要件が遡及適用されて直ちに系統接続が出来なくなることはない。**



（参考）要件適用の対象案件について

（IP通信機能を持たない機器は対象外）

- **IP通信機能を持たない機器**については、IoT製品のセキュリティラベリング制度であるJC-STAR★１の対象とならず、**今回の要件化の対象外**。ただし、IP通信機能を具備しており**IP通信の使用を予定していない機器**については、**IP通信機能を持つ場合はJC-STAR★１の取得が必要。**

（既設の対象設備を増設する際の取扱い）

- 既設の対象設備を**増設**する際（例：太陽光発電に蓄電池を増設）は、**増設部分に使用する対象機器は、JC-STAR★１取得製品の使用が必要**。既設の対象設備に使用している対象機器については、**機器交換をせずにそのまま使用する場合**は、**JC-STAR★１取得製品への交換は求めない。**

（FIP転／卒FIT案件の取扱い）

- FIP転に係る認定申請自体ではJC-STAR★1への対応を求めるものではない。
- 既存のFIT認定案件がFIP制度への移行（いわゆるFIP転）を行う場合や、 FIT/FIP認定案件が調達期間/交付期間の終了（いわゆる卒FIT）を迎える場合、**設備の増設や変更を伴わない場合**は、**JC-STAR★１取得製品への交換は求めない**。リパワリングやリプレースを伴う場合は、**更新する対象機器について、JC-STAR★１取得製品の使用が必要**。

（参考）要件適用の対象案件について

（機器故障等による機器交換時の対応が事業者に過度な負担となる場合の取扱い）

- 原則、2027年４月以降に対象機器をIP通信機能を有する機器に交換する場合及び既設の対象設備が採用する対象機器又はその一部を増設又は交換し、当該機器がIP通信機能を有する場合は、**増設又は交換する機器についてJC-STAR★１取得製品の使用が必要**。

  ただし、その時点でJC-STAR★1取得製品への交換を求めることにより、発電事業の継続に大きな影響を及ぼす等、**事業者に過度な負担が生じると属地の一般送配電事業者が認める場合**には、次の３点に関して、所定の様式により個別に協議を行い一般送配電事業者の了承を得ることを条件として、**当面の間、JC-STAR★１取得製品への交換を猶予する**。

①JC-STAR★1取得製品への交換が難しい理由及び「過度な負担」の具体的内容。

②当該対象設備の広範なリプレース／リパワリングの実行予定時期とJC-STAR★１取得製品への交換を実行する具体的な計画。

③それまでの間、事業者において講じるサイバーセキュリティ対策の内容。具体的には、「電力制御システムに関するサプライチェーン・セキュリティ対策の手引き」、「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」の利用、若しくはこれらと同等のサイバーセキュリティ対策。

電力サイバーセキュリティ対策に関するウェブサイトの開設

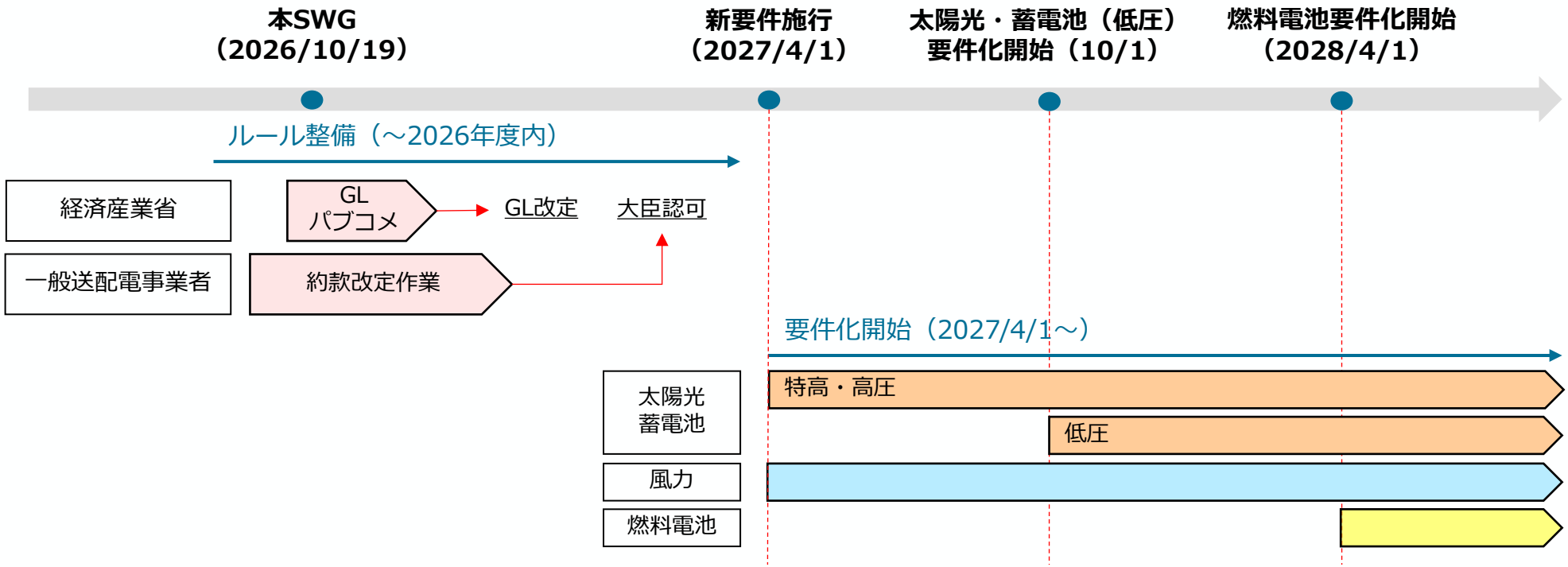
- グリッドコード検討会（主催：広域機関）での方針決定後、様々な事業者からの問合せを受け、FAQを含む最新の情報について、資源エネルギー庁のウェブサイト内にある電力サイバーセキュリティ対策に関するウェブページにて周知・広報を行っている。



こちらのQRコードより
アクセス可能です

JC-STAR★1要件化に向けた今後のスケジュール

- 「電力品質確保に係る系統連系技術要件ガイドライン」は年内を目途に改定予定。
- 各一般送配電事業者は、本ガイドラインを参照する形で系統連系技術要件（託送供給等約款別冊）を改定し、年度内に経済産業大臣に認可を申請予定。



今後の検討予定と本日ご議論いただきたい事項

今後の検討予定

- JC-STAR★１は一般的なIoT製品に求められる最低限度のセキュリティ水準を求めるもの。**電力分野固有の脅威や特性を考慮したサイバーセキュリティ対策**として、IoT製品類型ごとの特徴に応じた適合基準である**JC-STAR★２以上の策定に向けて、経済産業省においてIPAとも相談しながら検討準備を進めている**ところ。
- 今回JC-STAR★１取得要件化の対象となっていない、**風力発電におけるファイアウォール以外の機器**についても、追加の**適用対象や適用開始時期について広域機関のグリッドコード検討会で議論していく**。
- また燃料電池とともに検討していた**ガスエンジン**については、本年７月の英国の小規模ガス火力発電設備に対するサイバーインシデントも踏まえ、**改めて対象範囲を精査した上で広域機関のグリッドコード検討会にて議論する**。

これらの要件化を検討する上では、サイバーセキュリティの確保と同時に、**供給力の確保の観点からもバランスの取れた制度設計が必要**。今後、太陽光・蓄電池・燃料電池・風力**以外**で**追加すべき対象電源・機器の検討**を進めていくにあたり、**実効性のある対策を講じていくために留意すべき点**についてご意見をいただきたい。

（参考）英国の小規模発電設備における サイバーインシデントに関する報道

- 2026年7月、英国の小規模発電設備においてサイバーインシデントが発生し、操業を４日間停止していたと報道があった。詳細な情報はこれまで英国政府から公表されていないが、一部の報道によれば、今回影響を受けた発電設備は小規模ガス火力と言われている。英国の広域的なエネルギーシステムへのリスクはなかったとの英国政府のコメントが報じられている。

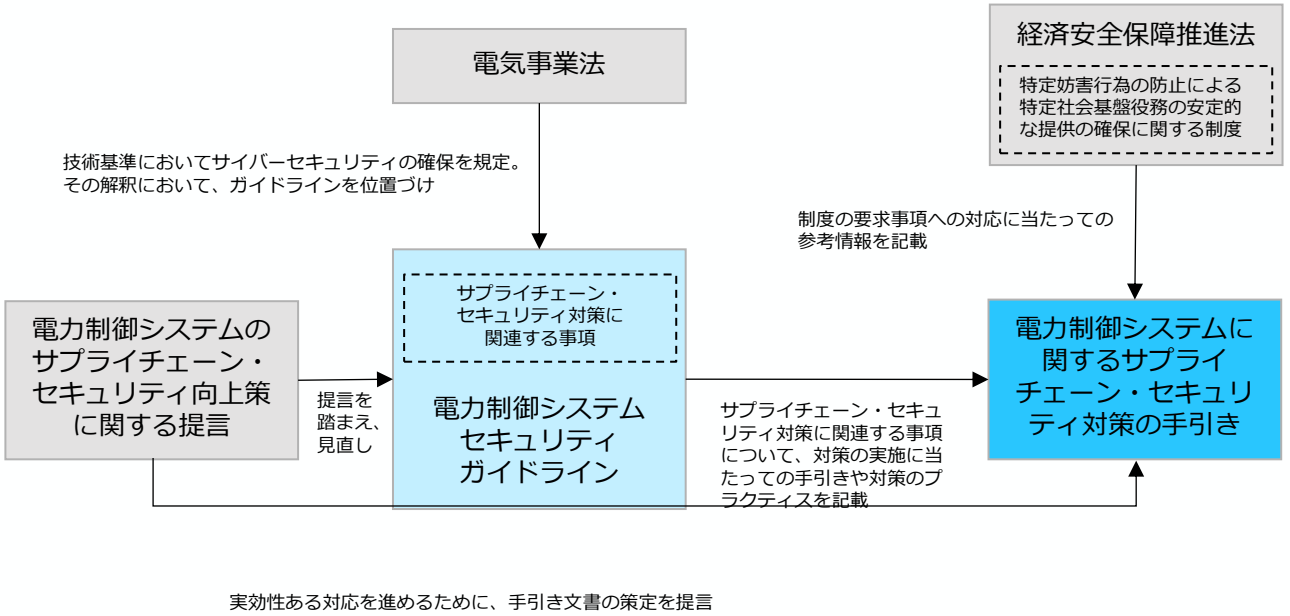
事案の概要（いずれも報道ベース）

発生時期	2026年7月
対象設備	英国の小規模発電設備。施設名、所在地、所有者は非公表
電源種・規模	小規模（約15MW）ガス火力発電設備 ※電力需要のピーク時間帯のみ稼働する前提の設備
被害	サイバー攻撃により4日間停止 ※停止に至った具体的な理由が攻撃によるものかどうかは不明

（出所）Iranian hackers shut down UK power plant , The Telegraph , 2026年8月22日　等の各種報道

（参考）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。



実効性ある対応を進めるために、手引き文書の策定を提言

目次

1.背景と目的
- 1.1.背景・目的
- 1.2.本文書におけるサプライチェーン・リスク
- 1.3.サプライチェーン・セキュリティ対策の重要性
- 1.4.本文書の位置づけ
- 1.5.主な対象読者・活用方法
- 1.6.本文書における「委託先等」の範囲

2.求められるサプライチェーン・セキュリティ対策
- 2.1.求められるサプライチェーン・セキュリティ対策
- 2.2.想定される対応プロセス

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
- 3.2.「2.セキュリティ仕様の確認」に関する対策の手引き・プラクティス
- 3.3.「3.機器の適切な管理」に関する対策の手引き・プラクティス

4.付録

（参考）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。

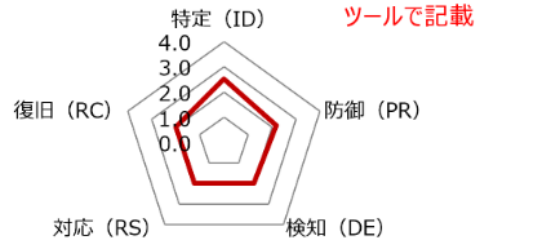
1. 背景・目的
2. 本ガイド・対策状況可視化ツールの構成
3. 本ガイド・対策状況可視化ツールの対象
4. 本ガイド・対策状況可視化ツールの想定活用方法
5. リスク点検項目・対策を怠った場合のリスク
6. リスク点検結果を踏まえた対策の改善方針
7. 参考文書
8. 用語集

＋

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



２．高性能AI等の技術革新に対する対応について

高性能AIによるソフトウェア脆弱性の早期発見

- ４月７日、米国アンソロピック社がソフトウェアの**脆弱性※の検査について高い能力**を有する汎用型次世代フロンティアAIの**Claude Mythos Preview**を発表。
- ソフトウェアの脆弱性については、これまで発見に数週間～数か月かかっていたものが、**Mythosでは数分～数時間で発見可能**、かつ、**人間では発見困難だった脆弱性も発見可能**となる。
- なお、Mythosに限らず、脆弱性の検査に係る高性能AIとしては、これまでもGoogle（BigSleep）やOpenAI（Codex Security、GPT-5.4-Cyber）等によっても開発・公表されている。

※脆弱性とは、プログラムのバグや設計上のミスが原因で発生するセキュリティ上の弱点。**サイバー攻撃の「入口」となる**ため、**脆弱性が残された状態でシステム等を利用していると、外部から攻撃を受ける等の危険性**がある。そのため、**脆弱性が発見された場合は、修正プログラム（パッチ）の適用やアップデートによる迅速な対策が必要。**
※脆弱性が公開されてから、パッチ適用等をする前に、当該脆弱性を利用して攻撃される脅威も存在。

- こうした高性能AIについては、未知の脆弱性の発見・是正の加速にも繋がり、ソフトウェアの開発者・提供者が有効に活用することで、**社会全体のサイバーセキュリティの向上につながることが期待。**
一方、悪意ある者に用いられた場合、脆弱性に対応できていない組織への**侵入リスクが高まる懸念**も。
- 特に、重要インフラ事業者については、サイバー攻撃によって、**情報の窃取のみならず、事業活動の停止やインフラの機能停止にもつながり得る**ことから、**上述したリスクには徹底した対応が必要。**

高性能AIへの対応に関する赤澤経済産業大臣と重要インフラ事業者との意見交換

- 経済産業省は、５月１日に電気事業連合会、送配電網協議会、日本ガス協会、石油化学工業協会、日本クレジット協会、石油連盟、電力分野の重要インフラ事業者（計24社）等との意見交換を実施。
- 会談では高性能AIの出現を踏まえた影響と重要インフラ分野（電力、ガス、化学、クレジット、石油）におけるリスク低減の観点から必要な対応について、関係者で認識を共有し、**以下の１～３の対策に取り組むことを依頼**。電力分野については、追加で自社のIT基盤や資産の把握と状況確認が依頼された。

１．組織のトップが主導して取り組むこと

：サイバーセキュリティリスクは経営リスクとの認識を持って、経営陣のリーダシップの下、必要なリソースの確保と対応を行う。

２．発見された脆弱性に早期に対応すること

：積極的に**脆弱性関連情報を収集**し、脆弱性が発見された場合には、リスク評価に基づき優先度を設定した上で、**重大度に応じて速やかに対応**すること。VPN機器等の導入・継続利用の要否について定期的に見直すことも必要。

３．基本的な対策に加えて「ゼロトラスト」への移行を進めること

：侵入口になり得る領域の縮小、ネットワークや端末の検知・監視、多要素認証、バックアップの確保といった**基礎的な対策に加え**、内部システム内のあらゆる挙動を常に確認する**「ゼロトラスト」に基づくシステム設計・運用への移行**を進める。また、**取組を実践する人材の育成**として、**IPAの「中核人材プログラム」の活用を検討いただきたい。**



高性能AIに関する政府の対策パッケージ（Project YATA-Shield）

* Yielding Advanced Threat Awareness with AI

- ５月18日、フロンティアAIモデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、**政府全体としての対策パッケージを取りまとめ。**

基本的な認識・考え方

重要インフラ事業者等・政府機関等が取るべき対応

- **発見された脆弱性のパッチ適用やリスク緩和措置**を速やかに実施（リスクベース）
- **基本的な対策、多層防御の実施、インシデント発生時の備え**　等

※英国・米国政府の注意喚起も参考に

脆弱性を発見するAIの進化

- **Anthropic（Project Glasswing）**：Mythosへのアクセスを、**ビッグテックや重要インフラ等**に限定。
- **OpenAI**：GPT-5.5-Cyberへのアクセスを、**一部の認証者**に限定して付与。

実施する施策

重要インフラ事業者等・政府機関等への対応

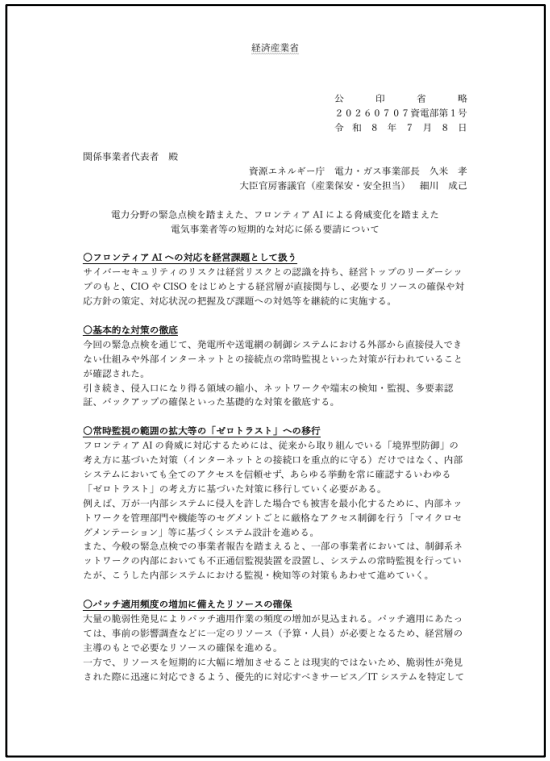
① **重要インフラ事業者等への注意喚起等**
② **金融分野での先行的な取組 及び 他分野への展開**
③ **人材育成支援**
④ **政府機関等の情報システムにおける対応**

脆弱性の発見・修正等への対応

① **外国政府機関やビッグテック等との更なる連携**
② **ソフトウェア・ベンダへの注意喚起**
③ **AISIによる技術支援等**
④ **技術開発の推進**
⑤ **高性能AIを活用したサイバー対処能力強化**

AIの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

- 電力分野の重要インフラ事業者におけるIT基盤・資産の点検の結果、高性能AIの脅威に対応するためには、より迅速なパッチ適用やそれに対応する体制整備の必要性が認識された。
- これを踏まえ、**本年７月、経済産業省・資源エネルギー庁から、「ゼロトラスト」への移行の具体化やパッチ適用頻度の増加に備えたリソースの確保等の追加対策を要請。**



経済産業省

公　印　省　略
２０２６０７０７資電部第１号
令　和　８　年　７　月　８　日

関係事業者代表者　殿

資源エネルギー庁　電力・ガス事業部長　久米　孝
大臣官房審議官（産業保安・安全担当）　福川　成己

電力分野の緊急点検を踏まえた、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について

○フロンティアAIへの対応を経営課題として扱う
サイバーセキュリティのリスクは経営リスクとの認識を持ち、経営トップのリーダーシップのもと、CIOやCISOをはじめとする経営層が直接関与し、必要なリソースの確保や対応方針の策定、対応状況の把握及び課題への対処等を継続的に実施する。

○基本的な対策の徹底
今回の緊急点検を通じて、発電所や送電網の制御システムにおける外部から直接侵入できない仕組みや外部インターネットとの接続点の常時監視といった対策が行われていることが確認された。
引き続き、侵入口になり得る領域の縮小、ネットワークや端末の検知・監視、多要素認証、バックアップの確保といった基礎的な対策を徹底する。

○常時監視の範囲の拡大等の「ゼロトラスト」への移行
フロンティアAIの脅威に対応するためには、従来から取り組んでいる「境界型防御」の考え方に基づいた対策（インターネットとの接続口を重点的に守る）だけではなく、内部システム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確認するいわゆる「ゼロトラスト」の考え方に基づいた対策に移行していく必要がある。
例えば、万が一内部システムに侵入を許した場合でも被害を最小化するために、内部ネットワークを管理部門や機能等のセグメントごとに厳格なアクセス制御を行う「マイクロセグメンテーション」等に基づくシステム設計を進める。
また、今般の緊急点検での事業者報告を踏まえると、一部の事業者においては、制御系ネットワークの内部においても不正通信監視装置を設置し、システムの常時監視を行っていたが、こうした内部システムにおける監視・検知等の対策もあわせて進めていく。

○パッチ適用頻度の増加に備えたリソースの確保
大量の脆弱性発見によりパッチ適用作業の頻度の増加が見込まれる。パッチ適用にあたっては、事前の影響調査などに一定のリソース（予算・人員）が必要となるため、経営層の主導のもとで必要なリソースの確保を進める。
一方で、リソースを短期的に大幅に増加させることは現実的ではないため、脆弱性が発見された際に迅速に対応できるよう、優先的に対応すべきサービス／IT システムを特定して

【要請内容の柱建て】

- フロンティアAIへの対応を経営課題として扱う
- 基本的な対策の徹底
- 常時監視の範囲の拡大等の「ゼロトラスト」への移行
- パッチ適用頻度の増加に備えたリソースの確保
- パッチ適用以外の脆弱性への対策の強化
- サイバーセキュリティ対策へのフロンティアAI等のAIの活用に向けた準備
- 他業界・業界内での連携の維持・強化

（参考）７月に実施したフロンティア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（１／３）

○フロンティアAIへの対応を経営課題として扱う

サイバーセキュリティのリスクは経営リスクとの認識を持ち、経営トップのリーダーシップのもと、CIOやCISOをはじめとする経営層が直接関与し、必要なリソースの確保や対応方針の策定、対応状況の把握及び課題への対処等を継続的に実施する。

○基本的な対策の徹底

今回の緊急点検を通じて、発電所や送電網の制御システムにおける外部から直接侵入できない仕組みや外部インターネットとの接続点の常時監視といった対策が行われていることが確認された。
引き続き、侵入口になり得る領域の縮小、ネットワークや端末の検知・監視、多要素認証、バックアップの確保といった基礎的な対策を徹底する。

○常時監視の範囲の拡大等の「ゼロトラスト」への移行

フロンティアAIの脅威に対応するためには、従来から取り組んでいる「境界型防御」の考え方に基づいた対策（インターネットとの接続口を重点的に守る）だけではなく、内部システム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確認するいわゆる「ゼロトラスト」の考え方に基づいた対策に移行していく必要がある。
例えば、万が一内部システムに侵入を許した場合でも被害を最小化するために、内部ネットワークを管理部門や機能等のセグメントごとに厳格なアクセス制御を行う「マイクロセグメンテーション」等に基づくシステム設計を進める。
また、今般の緊急点検での事業者報告を踏まえると、一部の事業者においては、制御系ネットワークの内部においても不正通信監視装置を設置し、システムの常時監視を行っていたが、こうした内部システムにおける監視・検知等の対策もあわせて進めていく。

（参考）７月に実施したフロンティア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（２／３）

○パッチ適用頻度の増加に備えたリソースの確保

大量の脆弱性発見によりパッチ適用作業の頻度の増加が見込まれる。パッチ適用にあたっては、事前の影響調査などに一定のリソース（予算・人員）が必要となるため、経営層の主導のもとで必要なリソースの確保を進める。

一方で、リソースを短期的に大幅に増加させることは現実的ではないため、脆弱性が発見された際に迅速に対応できるよう、優先的に対応すべきサービス／ITシステムを特定しておくとともに、委託先のベンダーの体制の確認、SSVCやKEVなどを参考にリスクベースでの脆弱性対応の優先順位付けを行う。

○パッチ適用以外の脆弱性への対策の強化

パッチ適用そのものが困難である場合や、パッチ適用に要する期間の短縮が困難な場合には、多層防御の強化や内部侵入時の横展開防止対策を講じる。

また、フロンティアAIの出現による脅威変化等を踏まえた最新のリスクに対応できるよう、レガシーシステムのアップグレードに向けた計画を進めるとともに、そのために必要な予算等のリソースを確保する。

さらに、各種対策を徹底してもサイバー攻撃を防御できない可能性を前提に、ITシステムの障害や停止への備え、能動的サービス停止の判断基準・手順を明確化する。

（参考）７月に実施したフロンティア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（３／３）

○サイバーセキュリティ対策へのフロンティアAI等のAIの活用に向けた準備

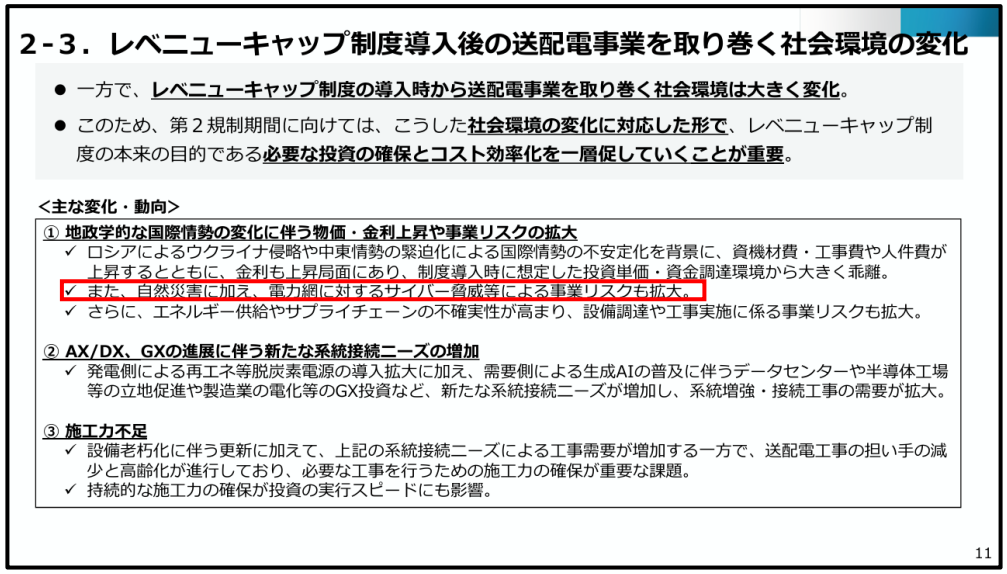
フロンティアAIなどのAIを活用したサイバーセキュリティ対策への準備を進めるため、 サイバーセキュリティ対策においてフロンティアAI等のAIを活用するシステムの範囲や情報管理体制、脆弱性管理プロセスなどの社内ルールの整備を進めるとともに、セキュリティ人材の確保や利用者教育を進める。

○他業界・業界内での連携の維持・強化

フロンティアAIに関する情報は短期間に多数公開されることから、自組織のみでの網羅的な把握は困難と想定される。このため、電力ISACや電力ISACを通じた他業界の ISAC、各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報の収集に努める。 また、自組織の取組を電力ISAC等の共助のためのコミュニティに積極的に共有し、電力分野全体の強靭性の向上に努める。

送配電事業におけるサイバーセキュリティ対策の強化

- 送配電事業者がこれらの要請に対応して必要なサイバーセキュリティ対策を講じるためには、**そのコストが託送料金収入において費用回収可能であることが必要。**
- 2028年度以降の託送料金収入の上限について検討する電力・ガス取引監視等委員会の審議会において、**送配電事業を取り巻く社会環境の変化**として**「電力網に対するサイバー脅威等による事業リスク」の拡大**が挙げられ、本年５月の経済産業大臣からの要請を含め、サイバーセキュリティ対策の重要性が取り上げられている。



2-3．レベニューキャップ制度導入後の送配電事業を取り巻く社会環境の変化

- 一方で、**レベニューキャップ制度の導入時から送配電事業を取り巻く社会環境は大きく変化**。
- このため、第２規制期間に向けては、こうした**社会環境の変化に対応した形で**、レベニューキャップ制度の本来の目的である**必要な投資の確保とコスト効率化を一層促していくことが重要**。

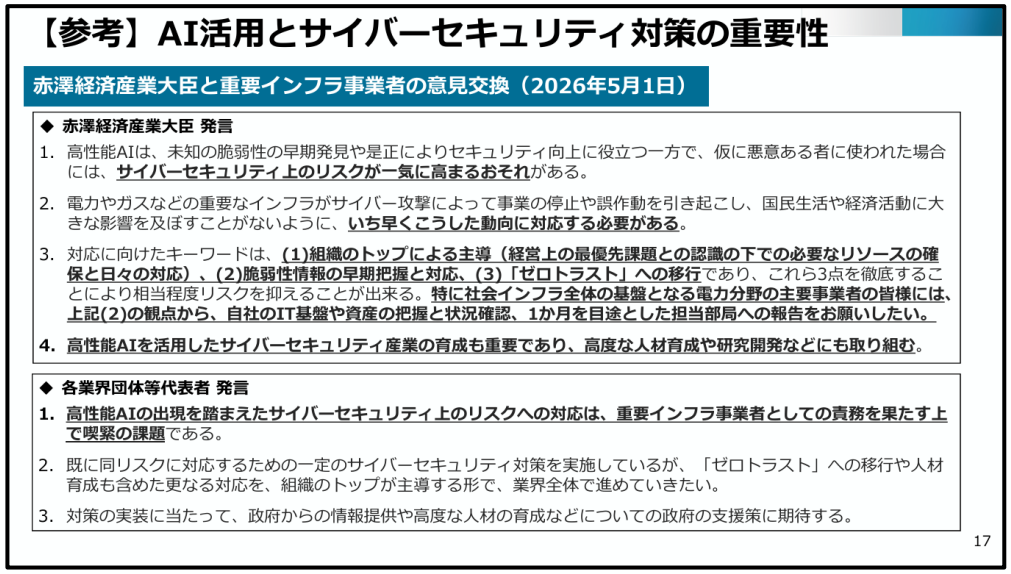
<主な変化・動向>

① 地政学的な国際情勢の変化に伴う物価・金利上昇や事業リスクの拡大
- ✓ ロシアによるウクライナ侵略や中東情勢の緊迫化による国際情勢の不安定化を背景に、資機材費・工事費や人件費が上昇するとともに、金利も上昇局面にあり、制度導入時に想定した投資単価・資金調達環境から大きく乖離。
- ✓ また、自然災害に加え、電力網に対するサイバー脅威等による事業リスクも拡大。
- ✓ さらに、エネルギー供給やサプライチェーンの不確実性が高まり、設備調達や工事実施に係る事業リスクも拡大。

② AX/DX、GXの進展に伴う新たな系統接続ニーズの増加
- ✓ 発電側による再エネ等脱炭素電源の導入拡大に加え、需要側による生成AIの普及に伴うデータセンターや半導体工場等の立地促進や製造業の電化等のGX投資など、新たな系統接続ニーズが増加し、系統増強・接続工事の需要が拡大。

③ 施工力不足
- ✓ 設備老朽化に伴う更新に加えて、上記の系統接続ニーズによる工事需要が増加する一方で、送配電工事の担い手の減少と高齢化が進行しており、必要な工事を行うための施工力の確保が重要な課題。
- ✓ 持続的な施工力の確保が投資の実行スピードにも影響。

11



【参考】AI活用とサイバーセキュリティ対策の重要性

赤澤経済産業大臣と重要インフラ事業者の意見交換（2026年5月1日）

◆ 赤澤経済産業大臣 発言

1. 高性能AIは、未知の脆弱性の早期発見や是正によりセキュリティ向上に役立つ一方で、仮に悪意ある者に使われた場合には、**サイバーセキュリティ上のリスクが一気に高まるおそれ**がある。
2. 電力やガスなどの重要なインフラがサイバー攻撃によって事業の停止や誤作動を引き起こし、国民生活や経済活動に大きな影響を及ぼすことがないように、**いち早くこうした動向に対応する必要がある**。
3. 対応に向けたキーワードは、**(1)組織のトップによる主導（経営上の最優先課題との認識の下での必要なリソースの確保と日々の対応）、(2)脆弱性情報の早期把握と対応、(3)「ゼロトラスト」への移行**であり、これら3点を徹底することにより相当程度リスクを抑えることが出来る。**特に社会インフラ全体の基盤となる電力分野の主要事業者の皆様には、上記(2)の観点から、自社のIT基盤や資産の把握と状況確認、1か月を目途とした担当部局への報告をお願いしたい。**
4. **高性能AIを活用したサイバーセキュリティ産業の育成も重要であり、高度な人材育成や研究開発などにも取り組む**。

◆ 各業界団体等代表者 発言

1. **高性能AIの出現を踏まえたサイバーセキュリティ上のリスクへの対応は、重要インフラ事業者としての責務を果たす上で喫緊の課題**である。
2. 既に同リスクに対応するための一定のサイバーセキュリティ対策を実施しているが、「ゼロトラスト」への移行や人材育成も含めた更なる対応を、組織のトップが主導する形で、業界全体で進めていきたい。
3. 対策の実装に当たって、政府からの情報提供や高度な人材の育成などについての政府の支援策に期待する。

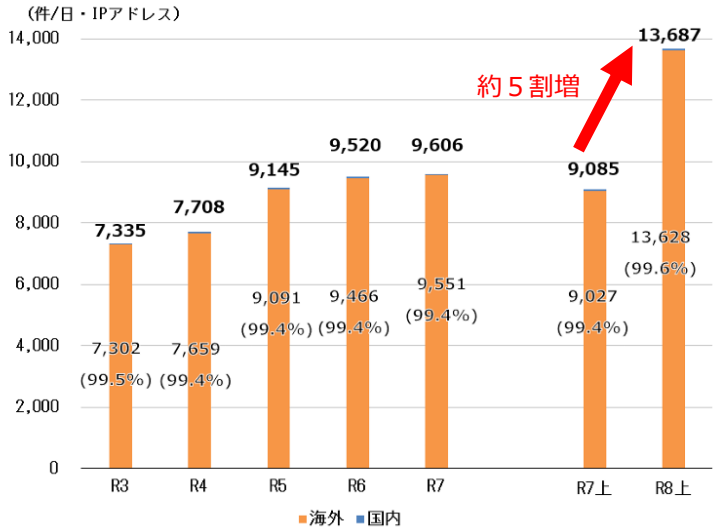
17

（出所）第78回料金制度専門会合（電力・ガス取引監視等委員会）資料１より

最近の不正アクセス事案への対応について

- 国内企業・組織において、不正アクセスに起因する情報漏えい等の被害が相次いで発生。
- こうした状況を踏まえ、本年10月9日、国家サイバー統括室（NCO）から、国内の事業者等に対し、ウェブシステム等の適切な管理、サプライチェーンを通じた侵害への対策、データの適切な管理などの対策の徹底を促す注意喚起を実施。
- 経済産業省としても、約1,000の業界団体を通じて、幅広く注意喚起を実施。

警察庁が検知した国内外からの不審なアクセス件数



出典：警察庁サイバー警察局「令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和８年９月）

「不正アクセスによる情報漏えい等の事案を踏まえた注意喚起及び情報提供に係る協力依頼」（10/9 経済産業省）

- 自社のみならず、**サプライチェーン全体でセキュリティを管理する**という認識の下、**①組織のトップによる主導**、**②脆弱性情報の早期把握と対応**、**③「ゼロトラスト」への移行**など、一層の対策の徹底を要請。
- サイバー攻撃による被害が発生した場合の**情報提供に係る協力**を依頼。
- 企業の皆様がサイバーセキュリティ対策を進める際に活用いただける**各種支援策を紹介**。

※NCO、JPCERT/CC、個情委からの注意喚起についてもあわせて周知。

（参考）サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）の実現

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策※1を提示しつつ、その状況を可視化する仕組み※2を構築（2026年３月27日に「制度構築方針」を公表）。
- 3段階の水準のうち、**★3・★４について、2026年度末の制度開始を目指し**、スキームオーナーであるIPAとともに、制度運営基盤の整備や利用促進等を進めていく。2026年度以降に**★５の設計も進める。**
- **制度開始５年後（2031年）までに２万件、10年後（2036年）までに５万件の★取得を目指す。**

※1　本制度では、サプライチェーンを構成する企業等のIT基盤が対象。
※2 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度

成熟度の定義	★ 3	★ 4	★ 5 [検討中※3]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

※3　ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

本日ご議論いただきたい事項

- 今回のSWGでは、電力分野の重要インフラ事業者に対する政府の要請を受けた各電気事業者の取組状況について、**電気事業連合会／電力ISAC及び送配電網協議会よりご報告**いただく。

  委員におかれては、国内外のサイバーセキュリティに関する今夏以降の状況変化や我が国の電力分野での対策状況を踏まえて、 **OT（制御系システム）とIT（事務系システム）の両面で実効性のある対策を講じていくために留意すべき点**についてご意見をいただきたい。

- 特に、直近では、**大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案が国内でも相次いで確認**されており、**経済産業省としても電力分野を含め関係業界への注意喚起を10月9日に実施**。海外では電力会社にも被害が生じているとの報道もある。

  これらのうち、**脆弱性の悪用やサプライチェーン（委託先企業等）を通じた侵害、アクセス権限等の情報管理の不徹底等が原因**と考えられるインシデントに対しては、**電気事業者に対してこれまで継続的に要請を行ってきた常時監視・多要素認証の導入、脆弱性対応の優先順位付け、委託先のベンダーの体制の確認、情報管理体制等の社内ルールの整備といった対策が有効**であると考えられるが、これら以外で**追加的に取り組むべき対策**があればご指摘いただきたい。

３．サイバー対処能力強化法及び整備法の施行について

サイバー対処能力強化法及び整備法の全体像（NCO資料より）

- 国家安全保障戦略（令和4年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

総　則
- 目的規定、基本方針等（第１章）

官 民 連 携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）←

アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日
公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

サイバー対処能力強化法及び整備法の施行

- サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるための「サイバー対処能力強化法（※１）及び同整備法（※２）」（昨年５月成立）が本年10月１日に施行。
- 既に重要な電子計算機を導入済みの事業者においては、施行後６か月以内での届出に向けた対応を行っている。

【電力分野の対応状況】

電力分野の基幹インフラ事業者49社（令和８年７月１日時点）に対しては、政府に対する

- ➢導入した一定の電子計算機の届出
- ➢インシデント情報の報告
- ➢情報共有・対策のための協議会への参加（任意）
- ➢協定に基づく通信情報の提供（任意）

が求められ、これらを通じて政府からの

- ➢脆弱性対応に必要な情報
- ➢提供された通信情報の分析結果の提供

を受けることができる。

※１：重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）
※２：重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）