資料5－1

系統用蓄電池事業を取り巻く
サイバーセキュリティリスクと対策の整理

三菱総合研究所

エネルギー・サステナビリティ事業本部

2025年 7月22日

目次

- 系統用蓄電池事業を取り巻くサイバーセキュリティリスク …… P．4
- サイバーセキュリティリスクへのあるべき対策の整理 …… P.13

本日の報告内容と目的

目的

- 系統用蓄電システムの導入が拡大する中、サイバーセキュリティリスクへの懸念が高まっている。
- 今後の政策の方向性を検討する上で、系統用蓄電池事業を取り巻くサイバーセキュリティリスクに対する正確な現状・課題の理解が重要である。
- ここでは、系統用蓄電池事業に内在するサイバーセキュリティリスクと各種関連規制等において定められている要件・項目を整理し、政策検討における論点を出すことを目的とした。

報告内容

1 系統用蓄電池事業を取り巻くサイバーセキュリティリスク

- 足元の状況や国内事業者・業界団体等へのヒアリングを通じて、サイバーセキュリティに関する現状の取組み・課題と想定されうる系統用蓄電事業者（蓄電所）へのサイバー攻撃を整理した。

2 サイバーセキュリティリスクへのあるべき対策の整理

- 蓄電所を構成する主なシステムの機能面及び国内事業者・業界団体等へのヒアリング結果を基に、系統用蓄電事業者（蓄電所）へのサイバー攻撃により想定されるリスクと対策を考察した。
- 国内外のサイバーセキュリティに関連する各種規制等を参照し、事業者等に求められる要件・項目を整理した。

系統用蓄電池事業を取り巻くサイバーセキュリティリスク

蓄電システム等におけるサイバー攻撃の脅威

- 分散型電源の導入拡大、デジタル化の進展等に伴い、サイバーセキュリティリスクへの懸念が高まっている。
- ジョージア大学の研究グループは、蓄電池システムにおける中国製部品のサイバーセキュリティリスクを指摘したホワイトペーパーを2024年6月に発表している。
- 我が国においては2024年5月に太陽光発電設備向け遠隔監視機器がサイバー攻撃の対象となり、不正に悪用されるといった事案が発生している。

サイバーセキュリティリスクへの懸念が示されている事例

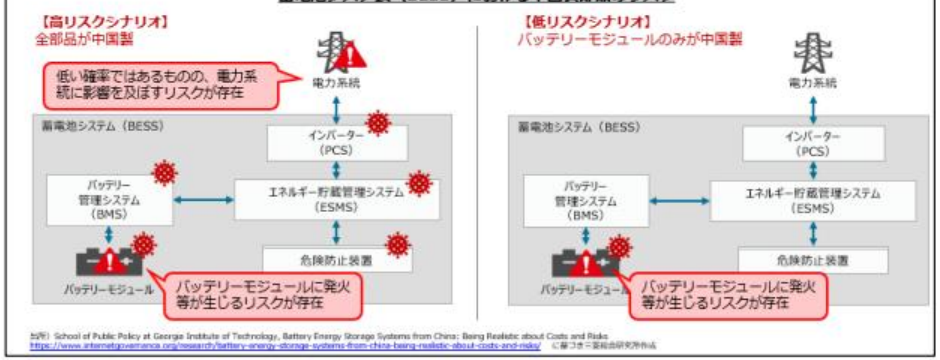
第17回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 電力サブワーキンググループ（2024年10月22日）資料4より

サプライチェーンを通じたサイバー攻撃の脅威等の事例

(2) 中国製蓄電池におけるサプライチェーン・リスクを指摘したホワイトペーパー

- 2024年6月、ジョージア工科大学の研究グループは、**蓄電池システム（BESS）における中国製部品のリスクを指摘したホワイトペーパー**を発表した。
- 全部品が中国製の場合（高リスクシナリオ）と、バッテリーモジュールのみ中国製（低リスクシナリオ）の両方について分析しており、**高リスクシナリオの場合、低い確率ではあるものの、電力系統に影響を及ぼすおそれがあると指摘**している。
- また、米国内では**中国製のバッテリーモジュールが主流である**ことから、**低リスクシナリオを避けることは困難であるとも指摘**している。

蓄電池システム（BESS）における中国製部品のリスク



出所）School of Public Policy at Georgia Institute of Technology, Battery Energy Storage Systems from China: Being Realistic about Costs and Risks
https://www.internetgovernance.org/research/battery-energy-storage-systems-from-china-being-realistic-about-costs-and-risks/ に基づき三菱総合研究所作成

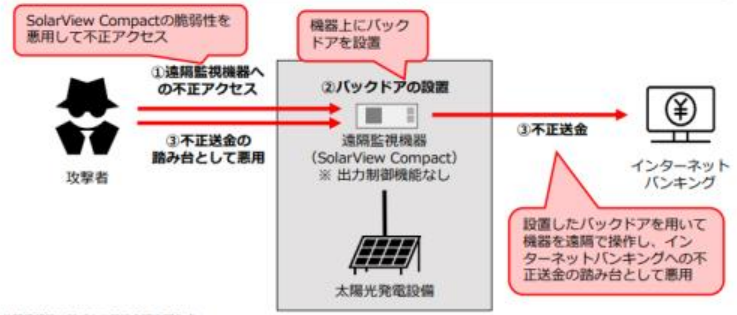
第17回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 電力サブワーキンググループ（2024年10月22日）資料５－１より

小規模太陽光発電設備に関する脅威事例

(1) 太陽光発電施設の遠隔監視機器800台におけるサイバー攻撃による乗っ取り・悪用

- 2024年5月、**太陽光発電設備向け遠隔監視機器の約800台がサイバー攻撃**を受け、**インターネットバンキングの不正送金に悪用**された。
- 攻撃を受けたのはコンテック社のSolarView Compactであり、同製品の**脆弱性が攻撃に悪用**された。同社は、対象製品は出力制御機能を有さないため、**系統への影響はない**としている。
- 同脆弱性は以前から報告されており、**複数の攻撃実証コード（PoCコード）も公開**されていた。

太陽光発電施設向け遠隔監視機器（SolarView Compact）に関連する一連のサイバー攻撃のイメージ



出所）以下の公開情報等に基づき三菱総合研究所作成
https://www.contec.com/jp/info/2024/2024050700/ ， https://www.trendmicro.com/ja_jp/jp-security/24/f/security-strategy-20240606-01.html

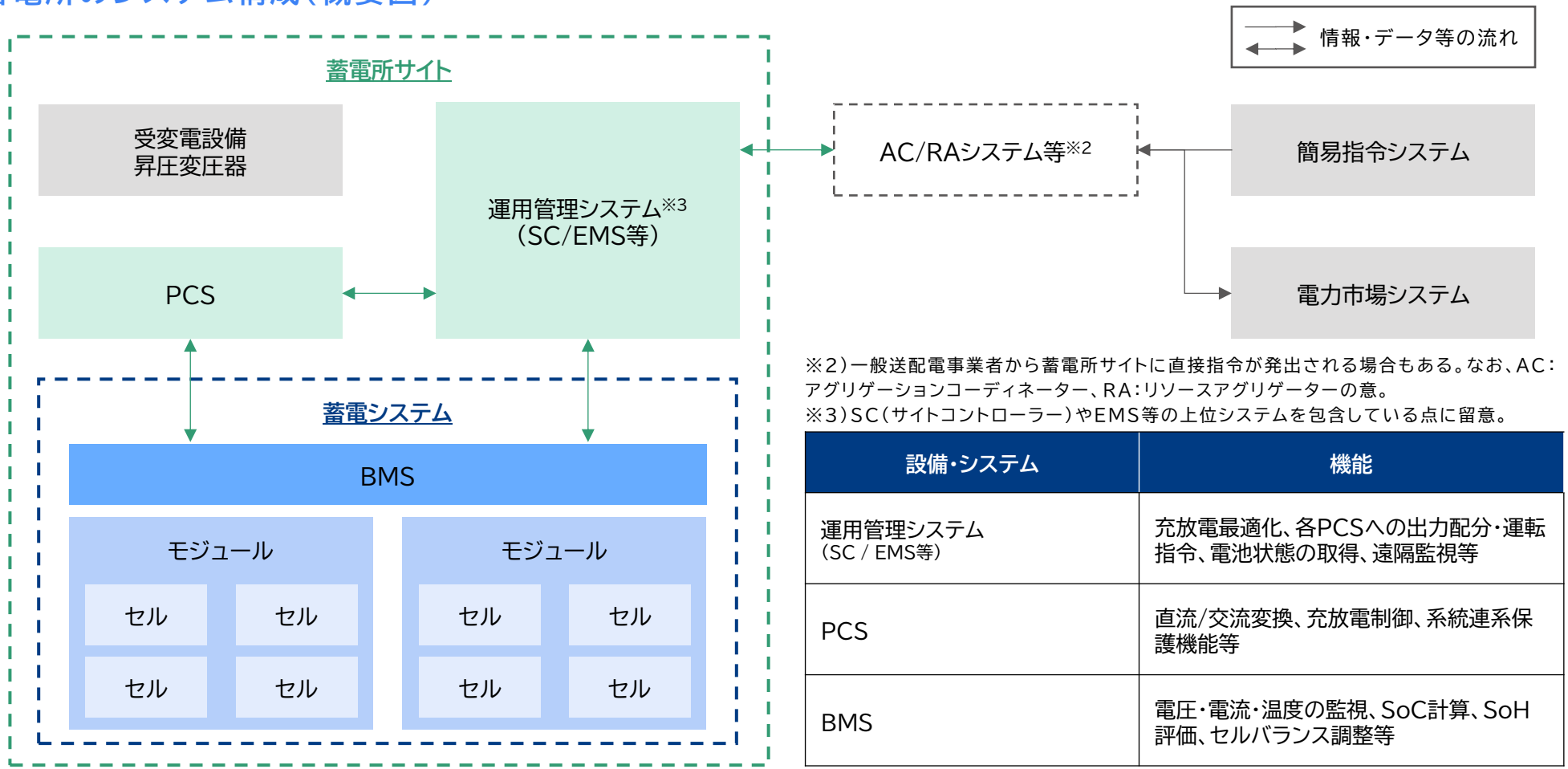
出所）資源エネルギー庁, 第104回 次世代電力・ガス事業基盤構築小委員会 制度検討作業部会｜資料3 “長期脱炭素電源オークションについて”, 閲覧日：2025年6月24日, https://www.meti.go.jp/shingikai/enecho/denryoku_gas/jisedai_kiban/system_review/pdf/104_03_00.pdf#page=34

蓄電所のシステム構成(1/2)

- 蓄電所は概ね以下のような設備にて構成されることが一般的である。
- BMS、PCS、運用管理システム(SC/EMS等)※1が蓄電所サイトにおける制御・監視を司るシステムであり、それぞれ電池状態の監視・評価、充放電制御、出力配分最適化等の機能を有している。

※1)BMS:バッテリーマネジメントシステム、PCS:パワーコンディショナー、SC:サイトコントローラー、EMS:エネルギーマネジメントシステム の略称。

蓄電所のシステム構成(概要図)



※2)一般送配電事業者から蓄電所サイトに直接指令が発出される場合もある。なお、AC:アグリゲーションコーディネーター、RA:リソースアグリゲーターの意。
※3)SC(サイトコントローラー)やEMS等の上位システムを包含している点に留意。

設備・システム	機能
運用管理システム (SC / EMS等)	充放電最適化、各PCSへの出力配分・運転指令、電池状態の取得、遠隔監視等
PCS	直流/交流変換、充放電制御、系統連系保護機能等
BMS	電圧・電流・温度の監視、SoC計算、SoH評価、セルバランス調整等

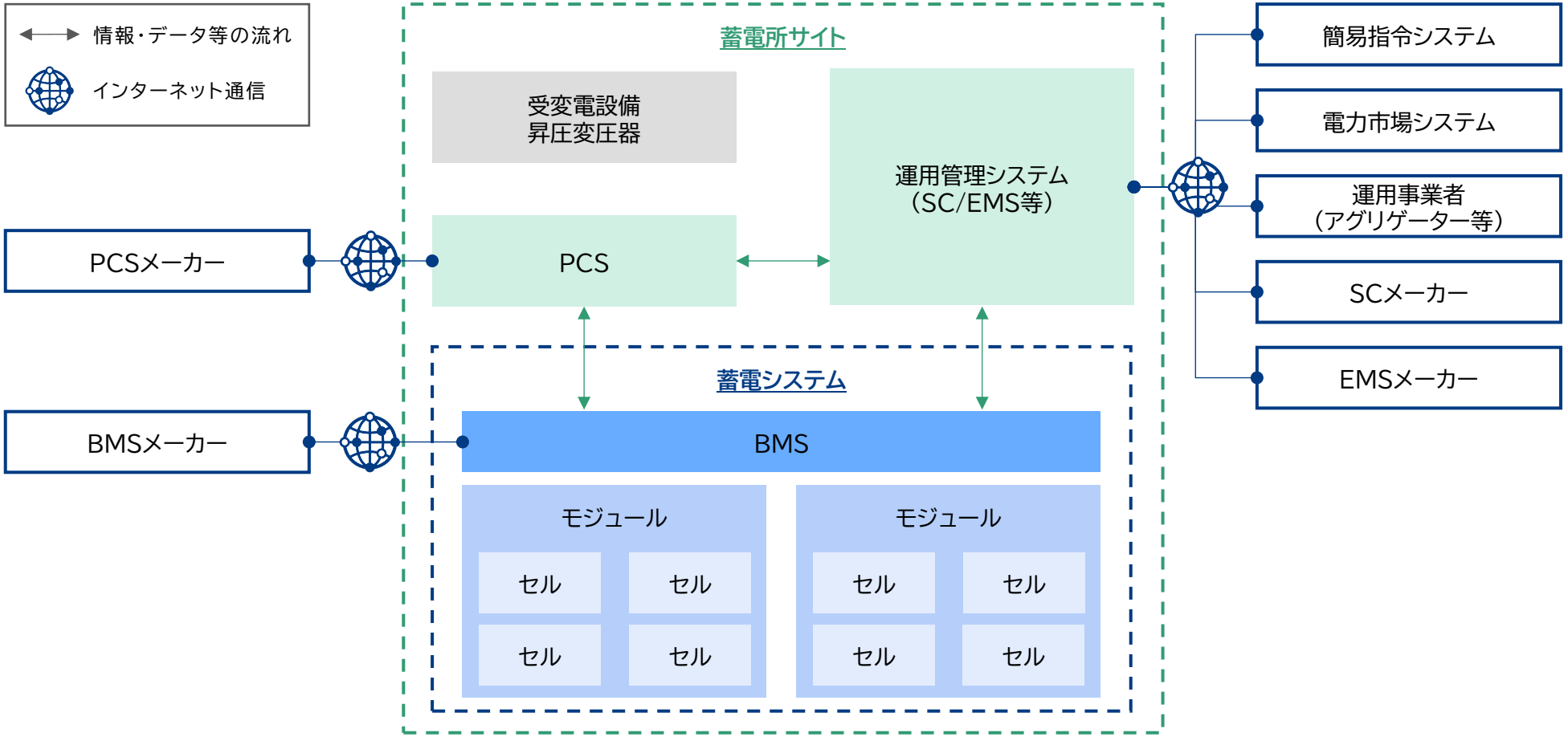
出所)資源エネルギー庁, 2024年度第2回 定置用蓄電システム普及拡大検討会｜資料4-6“系統用蓄電池の可能性と課題について(ERA)”, 閲覧日:2025年4月18日, https://www.meti.go.jp/shingikai/energy_environment/storage_system/pdf/2024_002_04_06.pdf 等より三菱総合研究所作成

蓄電所のシステム構成(2/2)

- 通信機能を有するBMS、PCS、運用管理システム※1は、メーカーや系統用蓄電池事業者による遠隔制御が可能であり、悪意のある第三者に通信が乗っ取られる等のサイバーセキュリティリスクが内在している。

※1)メーカー・機器によっては通信機能を有さないものもある点に留意。

蓄電所のシステム構成(概要図)



出所)資源エネルギー庁, 2024年度第2回 定置用蓄電システム普及拡大検討会｜資料4-6“系統用蓄電池の可能性と課題について(ERA)”, 閲覧日:2025年4月18日, https://www.meti.go.jp/shingikai/energy_environment/storage_system/pdf/2024_002_04_06.pdf 等より三菱総合研究所作成

蓄電所へのサイバー攻撃の想定パターン

- 蓄電所へのサイバー攻撃に関して、主体となりうるのは外部の第三者またはメーカー等の事業者である。
- 加えてサイバー攻撃の入口としては通信経由、あるいは設備・機器経由となることが想定されることから、以下の通り想定されうるサイバー攻撃のパターンを整理した。

蓄電所へのサイバー攻撃の整理

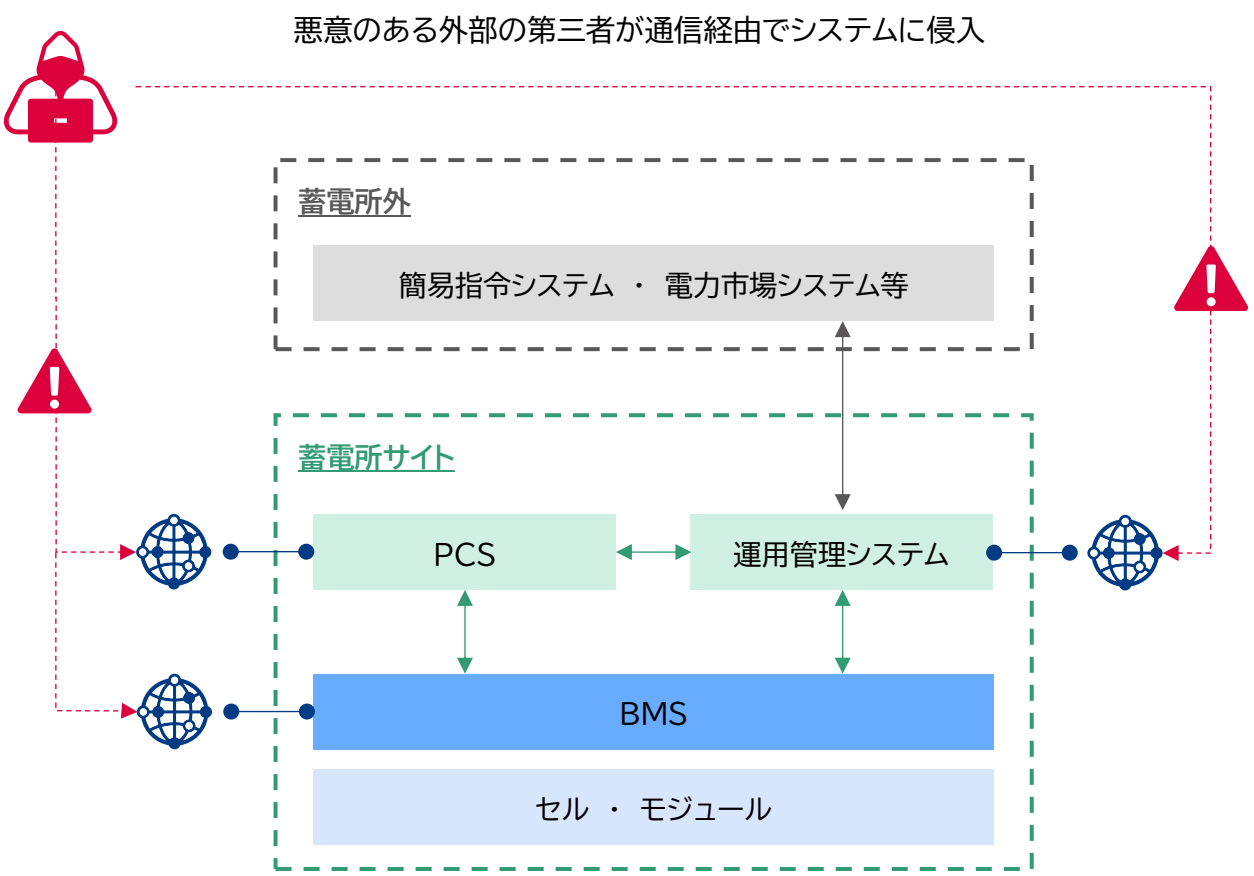
サイバー攻撃の主体 サイバー攻撃の入口	外部の悪意のある第三者	悪意のある事業者（メーカー等）
蓄電所の設備・機器等の通信を悪用するケース	パターン① • 外部の第三者による、通信経由でのサイバー攻撃 • 例えば、EMSやPCS等の通信が外部の第三者により乗っ取られるケースが想定される	パターン② • 蓄電所を構成するメーカー等の設備・機器が有する通信経由でのサイバー攻撃 • 例えば、悪意のあるメーカーが、自社のEMSやPCS等の通信を経由して、不適切な制御が行われる等のケースが想定される
蓄電所の設備・機器本体が脅威を有するケース※	外部の第三者の設備・機器が系統用蓄電システム（蓄電所）を構成することはないため考察は割愛	パターン③ • 蓄電所を構成するメーカー等の設備・機器本体が脅威を有するケース • 例えば、悪意のあるメーカーが自社のEMSやPCS等にバックドアを仕組み、不適切な制御が行われる等のケースが想定される

※）外部との間接的な通信などを通じて、設備全体に影響を及ぼす可能性のある設備・装置を含む。

想定される蓄電所へのサイバー攻撃(1/2)｜ 外部の第三者からの攻撃

- 悪意のある外部の第三者からのサイバー攻撃は、通信経由となることが想定される。
- 通信経由でBMS等のシステムに侵入し、データの改ざんや不正な制御が行われる可能性がある。

①悪意のある第三者による通信経由での攻撃



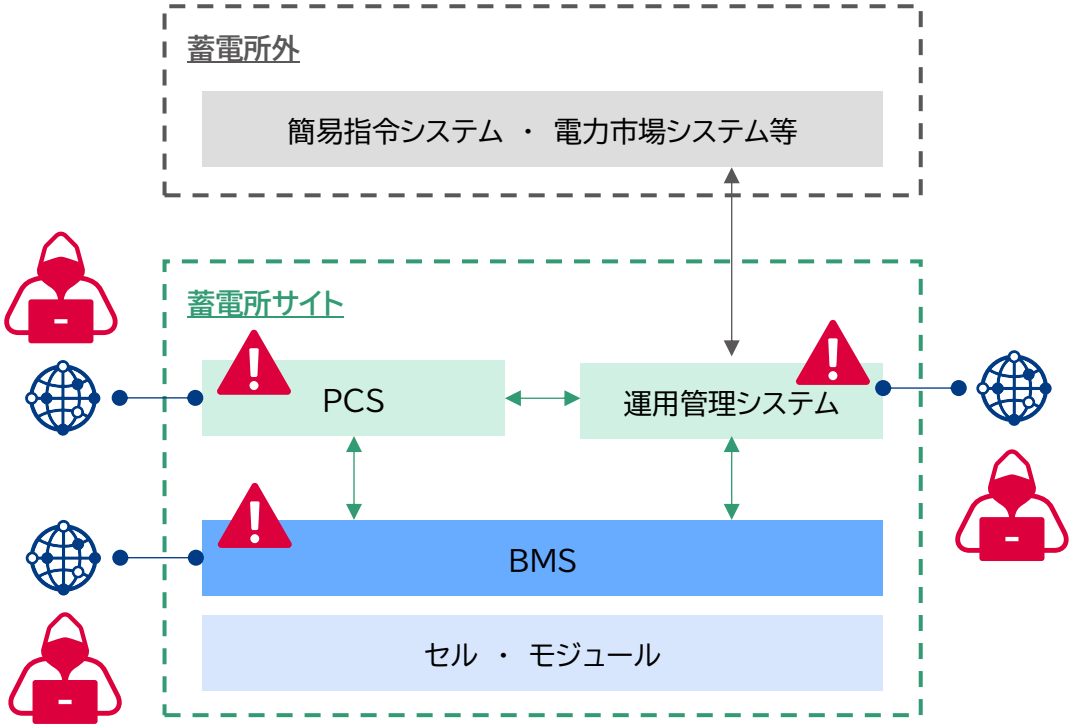
※）前頁のシステム構成図を簡略化して記載。

想定される蓄電所へのサイバー攻撃(2/2)｜ メーカーによる攻撃

- 悪意のある事業者(メーカー等)の機器がサイバー脅威を有しているケースが想定される。
- また、悪意のある事業者(メーカー等)が通信を介して機器にアクセスし、データ改ざんや不正操作をする可能性もある。

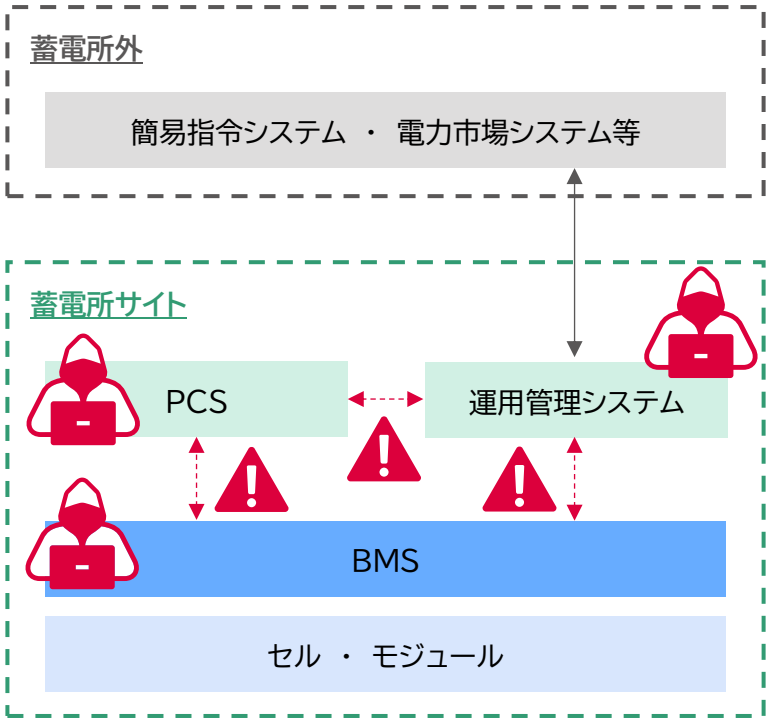
②悪意のあるメーカーによる通信経由での攻撃

悪意のあるメーカーが通信経由でシステムに侵入



③悪意のあるメーカーによる機器経由での攻撃

悪意のあるメーカーの機器がサイバー脅威を有している



※)前頁のシステム構成図を簡略化して記載。

系統用蓄電システム事業者へのヒアリング結果(1/2)

- 現状、ユーザー(系統用蓄電池事業者)からの仕様・要求に応じて、設備・機器メーカーは追加的にサイバーセキュリティ対策を実施している。
- また、サイバーセキュリティ対策の標準化や要件水準の面においては課題が確認された。

系統用蓄電池事業を取り巻くサイバーセキュリティリスクの現状

項目	ヒアリング結果
サイバーセキュリティに関する現状の取組み	● 設備・機器メーカーは、ユーザー(系統用蓄電池事業者)からの仕様・要求に応じてサイバーセキュリティ対策を追加的に講じている。 ● 設備・機器メーカー側からユーザー(系統用蓄電池事業者)に対して設備・機器のセキュリティ対策を積極的に説明することは稀である。 ● ユーザー(系統用蓄電池事業者)はガイドライン等のセキュリティ基準に適合し、要求する仕様を満たす設備・機器を選定し、納品後に仕様適合確認と作動試験を実施している。 ● JC-STAR★1やISMS27001認証のような第三者認証を取得している。 ● 蓄電所運転開始後の外部との通信(PCS等の蓄電所内の諸設備と製造メーカーとの通信)を制限している。 ● 定期的に第三者によるセキュリティ診断を実施している。 ● メーカーにERABに関するサイバーセキュリティガイドラインの内容に関するチェックシートの提出を求めている。
サイバーセキュリティに関する現状の課題	● サイバーセキュリティ対策は一定の水準で完結するものではないため標準化が難しく、かつ要件を厳格化するほどメーカー等の関連事業者は対応に時間・コストを要する。 ● 蓄電所のネットワーク構成は外部ネットワークとの接続口を一つのルーターに集約しているケースが多く、いずれかの設備・機器がサイバー攻撃を受けた場合、蓄電所内全体に影響が波及する可能性がある。 ● 蓄電所は電力市場取引を担う事業者と蓄電所オーナーが異なるケースがあり、セキュリティ対策の責任の所在が曖昧になりやすい。 ● 海外事業者を含めてPCSメーカーや蓄電池メーカーがどの程度社内のサイバーセキュリティ対策を実施しているか分からない。 ● 過剰なサイバーセキュリティ対策を求めると、蓄電所設置コストが大幅に増加してしまい、最終的には電気代等として国民負担の増加に繋がることにも留意が必要。

系統用蓄電システム事業者へのヒアリング結果(2/2)

- 蓄電所を構成する幅広い機器がサイバー攻撃のリスクに曝されている。
- ユーザー(系統用蓄電池事業者)にサイバー脅威の事例や有効な対策を周知するとともに、ガイドラインや補助制度等を通じて、一定水準を確保するための実効性ある対策の導入を求めていく必要がある。

系統用蓄電池事業を取り巻くサイバーセキュリティリスクの現状

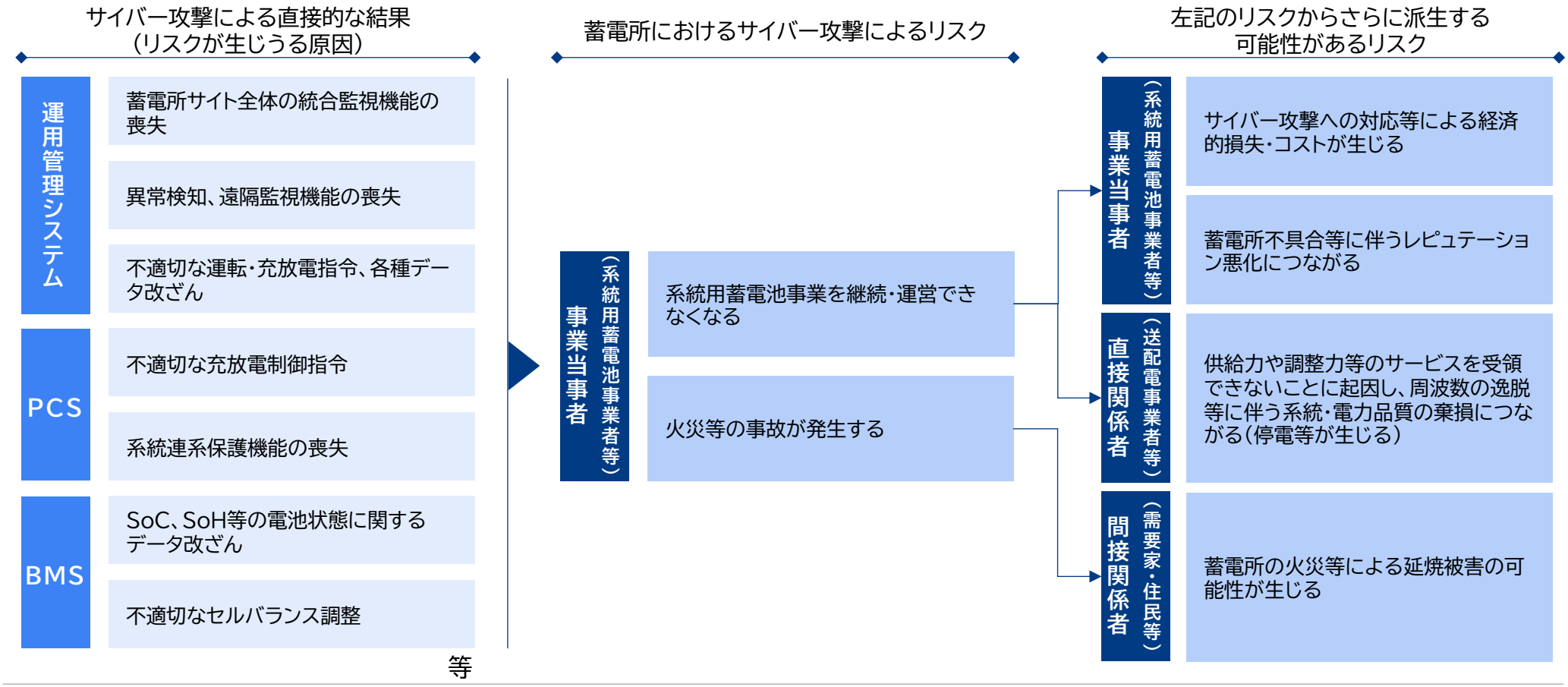
項目	ヒアリング結果
想定される蓄電所へのサイバー攻撃とリスク・影響	● EMS、PCS、BMSはネットワークに接続され遠隔操作が可能な設備・機器であることから、サイバー攻撃の対象となる。受変電設備等は閉域ネットワークで運用されるケースが多く、現状はサイバー攻撃の対象になりづらい。 ● オープンソースのOSを用いている設備は全て攻撃対象となり得る。 ● 蓄電所の運用停止をもたらす攻撃を想定すると、受変電設備の開閉器もサイバー攻撃の対象ではないか。 ● 上位クラウドシステムは複数の蓄電所との通信が可能であり、サイバー攻撃による影響度は大きいと考えられる。 ● 系統・電力品質への悪影響を防止するという観点においては、通信・遠隔操作機能を有する蓄電所内の全設備・機器にサイバーセキュリティ対策を講じる必要がある。 ● BMSを攻撃することで悪意ある制御を行うことは比較的難しいと考えられる。蓄電所の稼働停止等を目的に攻撃が行われる場合はEMS、SC、PCSが標的になる可能性が高い。
サイバーセキュリティに関する意見	● ユーザー(系統用蓄電池事業者)や設備・機器メーカーに対して、サイバー脅威の事例および対策として有効な手段に関する情報を提示することでサイバーセキュリティ対策の必要性の認識が進むのではないか。 ● 小規模事業者の対応が難しい内容や市場縮小につながりうるサイバーセキュリティ対策に関しては、対策に要するコストと得られる効果を精査して求められる対策の水準を決定していくべきではないか。 ● 系統用蓄電池事業に関連する各種電力システムのガイドラインを周知いただきたい。 ● 今年度、補助制度の要件やガイドラインにおいて、JC-STAR★1の認証取得をシステムを構成する全ての機器に求めることは、認証取得にかかる期間等を考慮すると難しいと思われる。 ● 攻撃箇所を最小限に抑えるべく、通信を一か所のGWに集約して、その部分のセキュリティ対策を万全にしておくのが適切な対応ではないか。 ● バックドア対策として、SCにレイヤー構造を設けることで、攻撃の影響を最小限に留めるようなシステムを構築すべきではないか。 ● クラウドに接続可能な担当者の社内の権限等の整理をガイドラインや補助制度において要件化することで業界全体として対策レベルが向上すると考える。 ● 蓄電所の増加に伴い、系統への影響も増大する。高圧と特高で必要なセキュリティレベルを分けるべきではないか。 ● PCS・BMS等とメーカーとの通信を、蓄電所側から切断できるような機能を具備することが必要ではないか。

サイバーセキュリティリスクへのあるべき対策の整理

蓄電所へのサイバー攻撃により想定されるリスク

- 蓄電所へサイバー攻撃が成功した場合、蓄電所の運転停止または火災等の事故の発生のリスクが生じる。
- さらに、事業当事者の経済的損失・レピュテーションリスク以外にも送配電事業者等の関係者や近隣住宅にも影響が派生する可能性がある。
- このような間接的な影響も踏まえ、社会的コスト最適化の観点から、関係者間でサイバー攻撃によるリスクのシェアと対応の在り方について検討することが求められる。

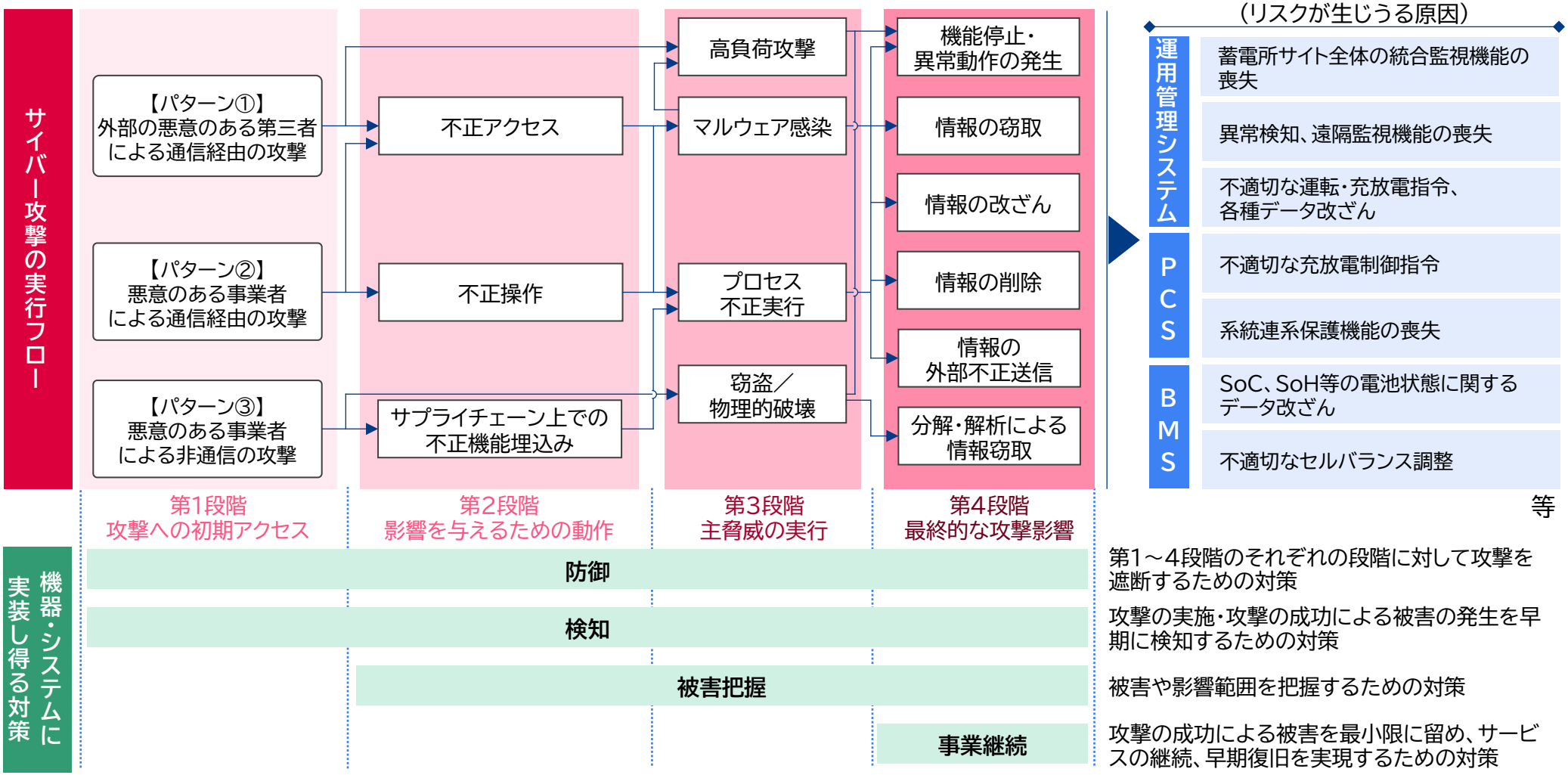
サイバー攻撃により想定されるリスク



蓄電所へのサイバー攻撃の実行フローと機器・システムに実装し得る対策

- 系統用蓄電池事業者は、蓄電所へのサイバー攻撃に対して防御・検知・被害把握・事業継続に資する対策を具備した機器・システムを選定・調達することが重要である。

サイバー攻撃の実行フローと系統用蓄電池事業者の機器・システムに実装し得る対策



出所）独立行政法人情報処理推進機構,制御システムのセキュリティリスク分析ガイド（2023年3月版）, 閲覧日：2025年7月14日, https://www.ipa.go.jp/security/controlsystem/riskanalysis.html 等を基に三菱総合研究所作成

【参考】系統用蓄電池事業者の機器・システムに実装し得る対策の内容

- 系統用蓄電池事業者の機器・システムに実装し得る対策の内容と対策例は下表の通り。

系統用蓄電池事業者の機器・システムに実装し得る対策内容と対策例

目的		説明	対策例
防御	第1段階	攻撃パターン①～③の初期段階を防止する目的で実装される対策。 また、攻撃者によるシステムへの不正ログイン等を防止する目的で実装される対策。	ファイアウォール アンチウイルス 通信相手の認証　等
	第2、3段階	システムへの侵入を果たした攻撃者による、内部の情報収集や侵入範囲の拡大を防止する目的で実装される対策。	セグメント分割/ゾーニング アクセス制御　等
	第4段階	「情報窃取」「データ改ざん」「システム破壊」等、攻撃者による最終目的の実現を防止する目的で実装される対策。	重要操作の承認 データ暗号化 フェールセーフ設計　等
検知		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策。	統合ログ管理システム 機器異常検知 侵入センサ　等
被害把握		攻撃の成功による被害や影響範囲の把握を目的に実装される対策。 あるいは、監査のための証跡刑事のため、攻撃内容の詳細の把握等を目的に実装する対策。	ログ収集・分析 統合ログ管理システム　等
事業継続		攻撃の成功による被害を最小限に留めるために実装される対策。 あるいは、サービスの継続、被害の早期復旧を実現することを目的に実装される対策。	データバックアップ 冗長化 暗号鍵更新　等

出所）独立行政法人情報処理推進機構,制御システムのセキュリティリスク分析ガイド（2023年3月版）, 閲覧日：2025年7月14日,
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html 等を基に三菱総合研究所作成

系統用蓄電池事業者に求められるセキュリティマネジメントの取組

- 前頁で整理した系統用蓄電池事業者の機器・システムに実装し得る対策の有効性を高めるため、系統用蓄電池事業者に求められるセキュリティマネジメントの取組を下記の通り整理。
- 必要十分なサイバーセキュリティ対策機能を具備した機器の調達以外にも、サイバーセキュリティリスクの管理体制の構築やインシデント発生時の体制の構築、関係者との継続的なコミュニケーション等の実施が求められる。

系統用蓄電池事業者に求められるセキュリティマネジメントの取組

系統用蓄電池事業者に求められるセキュリティマネジメントの取組	サイバーセキュリティリスクの管理体制構築	• リスクの認識・組織全体での対応方針の策定 • リスク管理体制の構築 • サイバーセキュリティ対策のための資源確保
	サイバーセキュリティリスクの特定と対策の実装	• リスクの把握とリスク対応に関する計画の策定 • リスクに効果的に対応する仕組みの構築 • サイバーセキュリティ対策の継続的改善
	インシデント発生に備えた体制構築	• インシデント発生時の緊急対応体制の整備 • インシデントに対する事業継続・復旧体制の整備
	サプライチェーンセキュリティ対策の推進	• 調達等におけるサプライチェーン上のサイバーセキュリティ対策の確認 • ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
	関係者とのコミュニケーションの推進	• サイバーセキュリティに関する情報の収集、共有及び開示の促進

※）本検討においては系統用蓄電池事業者に求められる取組を整理した。同様に、関係する事業者（送配電事業者、アグリゲーター等）において適切な取組や対策を講じることも重要である点に留意。

出所）経済産業省.サイバーセキュリティ経営ガイドライン Ver 3.0 , 閲覧日：2025年7月14日, https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf を基に三菱総合研究所作成

電力分野のサイバーセキュリティに関する各国の主な規制等

- 各国のサイバーセキュリティリスクに関する法規制及びガイドライン等として以下のようなものが挙げられる。

各国のサイバーセキュリティに関する主な規制等

	日本	米国	EU	英国
法規制	• 電気事業法	• NERC CIP • California Civil Code；Division3 Part4	• NIS 2 Directive • EU Cyber Resilience Act※2	• NIS regulation 2018 • Cyber Security and Resilience Bill※1 • UK Product Security and Telecommunications Infrastructure Act 2022；Part1
系統接続時の対策･要件等	• 系統連系技術基準	• FERC Order（No.706/791/802/850/866）	• EU network code on cybersecurity for the electricity sector（C/2024/1383）	• Grid Code
関連ガイドライン･認証制度等	• 電制GL • スマメGL • PCS技術仕様 • 自家用GL • 小売GL • ERAB GL • 特定卸供給の指針 • JC-STAR制度	• Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid（DoE） • Cyber Security for Distributed Energy Resources and DER Aggregators（NERC） • UL2941：Cybersecurity Certification Standard for DER and Inverter-based Resources（NREL/UL） • Product Security Verified Mark（CSA）		• ENA Distributed energy resources（DER）cyber security connection guidance

※1）2025年中に導入予定の新たなサイバーセキュリティ法案。現行のNIS規則を強化･拡大した内容が検討されている。
※2）2024年3月に欧州議会にて可決され2024年12月に正式発効。2027年頃から本格施行となる見込み。

国内外のサイバーセキュリティ関連規制等において定められる要件・項目

- サイバーセキュリティリスクへの懸念が高まる中、国内外の関連規制等では以下のような要件・項目が定められており、対象となる事業者に対策を求めている。

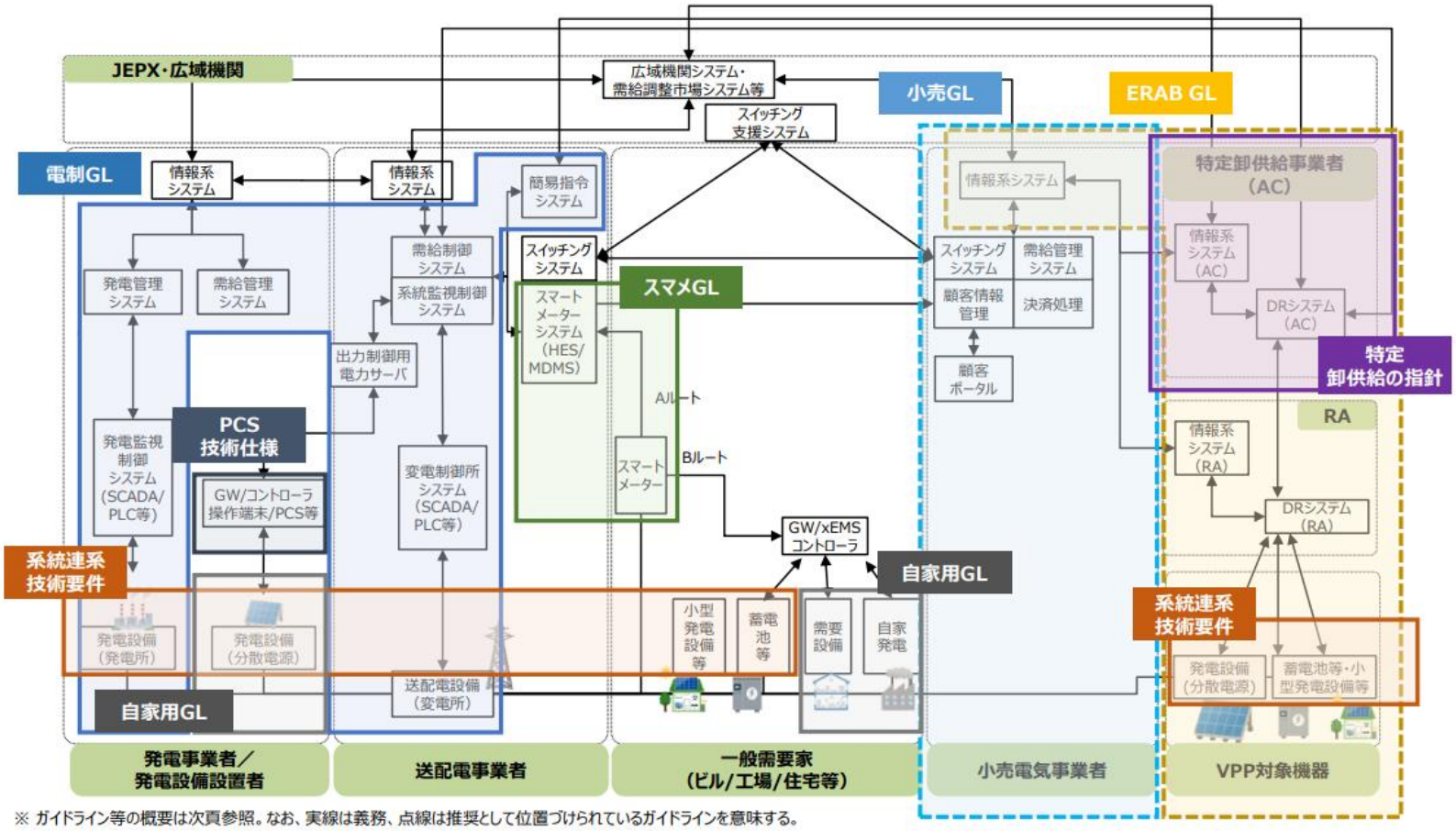
国内外のサイバーセキュリティ関連規制等において定められる要件

要件・項目の概要	対象となる規制・ガイドライン等
■ セキュリティの維持・管理 ■ 責任の明確化	• 日本 ： 電制GL、 特定卸供給の指針、 自家用GL、 PCS技術仕様 • 米国 ： NERC CIP、 DoE支援制度（インフラ投資雇用法の遵守） • EU ： Cyber Resilience Act • 英国 ： NIS regulation 2018
■ インシデント報告 ■ 対応・復旧計画の策定 （提出を求める場合もある）	• 日本 ： 電制GL、 特定卸供給の指針 • 米国 ： NERC CIP、 DoE支援制度（インフラ投資雇用法の遵守） • EU ： NIS2、 Cyber Resilience Act、 network code on cybersecurity for the electricity sector • 英国 ： NIS regulation 2018、 Cyber Security and Resilience Bill
■ サプライチェーンリスク管理 ■ 認証・規格等の取得	• 日本 ： 電制GL、 ERAB GL、 JC-STAR • 米国 ： NERC CIP、 Cybersecurity Considerations for DER on the U.S. Electric Grid、 UL2941 • EU ： NIS2、 Cyber Resilience Act、 network code on cybersecurity for the electricity sector • 英国 ： NIS regulation 2018、 Cyber Security and Resilience Bill
■ セキュリティ教育・訓練の実施	• 日本 ： 電制GL、 特定卸供給の指針 • 米国 ： NERC CIP、 DoE支援制度（インフラ投資雇用法の遵守） • EU ： NIS2、 network code on cybersecurity for the electricity sector

電力システムのサイバーセキュリティに関するガイドライン等

- 我が国における電力システムのサイバーセキュリティに関するガイドライン等は下図の通り整備されている。
- 各ガイドライン等が対象とするシステムの範囲は区分けされており、遵守が義務付けられているものもある。

電力システムのサイバーセキュリティに関するガイドライン等の概観



※ ガイドライン等の概要は次頁参照。なお、実線は義務、点線は推奨として位置づけられているガイドラインを意味する。

出所）三菱総合研究所, 令和4年度エネルギー需給構造高度化対策に関する調査等事業（電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）｜報告書, 閲覧日：2025年4月16日, https://www.meti.go.jp/meti_lib/report/2022FY/000269.pdf

各種ガイドラインと系統用蓄電池との関連性(1/2)

- 電気事業法、規制措置等における系統用蓄電池の取扱い等を踏まえ、ガイドライン等との関連性を整理した。

各種ガイドライン等と系統用蓄電システムとの関連性

名称	主な対象	発行主体	概要	系統用蓄電池との関連性
電力制御システムセキュリティガイドライン 電制GL	電気事業の用に供する電気工作物	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電気工作物に対しては、本ガイドラインに基づく対策が求められる。	10MW以上の系統用蓄電池は発電事業に該当することから本ガイドラインに基づく対策が求められる。
スマートメーターシステムセキュリティガイドライン スマメGL	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。	
系統連系技術要件 系統連系技術要件	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。	系統連系する発電設備に対してすべからく求められる技術要件であるため系統用蓄電池も対象となる。
出力制御機能付PCSの技術仕様 PCS技術仕様	出力制御機能付PCS	JPEA・JEMA・電事連	出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。	PCSは系統用蓄電池の構成設備に含まれることから対象となる。

出所)資源エネルギー庁, 電力分野におけるサイバーセキュリティについて, 閲覧日:2025年4月16日,
https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/073_07_00.pdf 等より三菱総合研究所作成

各種ガイドラインと系統用蓄電池との関連性（2/2）

- 系統用蓄電池のリソース所有者のみならず、アグリゲーターとして事業に関与する場合に対象となるガイドライン等もある。

各種ガイドライン等と系統用蓄電システムとの関連性

名称	主な対象	発行主体	概要	系統用蓄電池との関連性
自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規） 自家用GL	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。	1MW以上かつ10MW未満の系統用蓄電池は特定自家用電気工作物に該当。
小売電気事業者のためのサイバーセキュリティ対策ガイドライン 小売GL	小売電気事業者	資源エネルギー庁	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。	
ERABに関するサイバーセキュリティガイドライン Ver3.0 ERAB GL	ERABに関する事業者	経済産業省・IPA	ERABのサービスレベルを維持するためにERABに参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。	アグリゲーターとして系統用蓄電池ビジネスに参入する場合に加えて、アグリゲート対象となる系統用蓄電池を所有する場合も該当。
特定卸供給に係るサイバーセキュリティ確保の指針 特定卸供給の指針	特定卸供給事業に関するシステム	資源エネルギー庁	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。	アグリゲーターとして系統用蓄電池ビジネスに参入する場合は本指針に沿う必要がある。

出所）資源エネルギー庁，電力分野におけるサイバーセキュリティについて，閲覧日：2025年4月16日，
https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/073_07_00.pdf 等より三菱総合研究所作成

電力分野の制度・規制等におけるサイバーセキュリティの扱い(1/2)｜ 日本

- 国内の電力分野の制度・規制等に関しては、相互に解釈等を参照しつつ技術基準やサイバーセキュリティに関する要件が規定されている。
- 「ERABに関するサイバーセキュリティガイドライン」は2025年5月の改定において、新規導入のIoT製品についてはJC-STAR★1以上の取得を求めている。

電気事業法	系統連系技術要件	電力制御システムセキュリティガイドライン	ERABに関するサイバーセキュリティガイドライン
電気設備に関する技術基準を定める省令(電技省令)の中で、事業用電気工作物の運転を管理する計算機に対してサイバーセキュリティを確保する義務を規定。技術基準の解釈として、「自家用GL」、「スマメGL」、「電制GL」を参照。 **【技術基準の解釈として参照するGL】** 自家用GL スマメGL 電制GL	系統連系する発電設備にすべからく求められる要件であり、事業用電気工作物については「電制GL」、自家用電気工作物については「自家用GL」に準拠している。その他の発電設備等については、サイバー攻撃による異常防止、サイバー攻撃時の異常除去・影響範囲の局限化等の対策が求められる。 **【対策の概要】** ● ネットワーク接続点の保護 ● マルウェア対策 ● 系統運用者に対するセキュリティ管理責任者の通知	電気事業者が管理する電気設備やシステムに求められるセキュリティ機能及び運用・管理上の対策について、電気事業法に基づく保安規定の技術基準として定められたもの。電気事業者が実施すべきセキュリティ対策の要求事項を規定。 **【対策の概要】** ● 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 ● 定期的なセキュリティ診断とソフトウェア更新等の脆弱性管理 ● ベンダーや外部委託先等のサプライチェーンリスク管理 ● 異常な通信や動作をリアルタイムで監視し、迅速に対応できる体制の整備 ● サイバー攻撃を想定した対応計画の策定と訓練の実施	各種分散型エネルギーリソース(DER)、BEMS、HEMS等のエネルギーマネジメントシステム、DR・VPP関連機器・システムが対象。簡易指令システムやアグリゲーションコーディネーターが有するシステムは「電制GL」を参照している。 **【対策の概要】** ● IoT機器の脆弱性管理 セキュリティ適合性評価制度(JC-STAR制度)を参考にしたIoT機器の脆弱性管理対策を記載 ● アグリゲーターが取得する情報のリスクを考慮し、適切なデータ管理とプライバシー保護を推奨

出所)e-GOV, “電気事業法 令和6年4月1日 施行”, 閲覧日:2025年7月14日, https://laws.e-gov.go.jp/law/339AC0000000170/20250606_505AC0000000044#Mp-Ch_3
経済産業省, “電力品質確保に係る系統連系技術要件ガイドライン,令和6年12月1日”, 閲覧日:2025年7月14日,
https://www.enecho.meti.go.jp/category/electricity_and_gas/electric/summary/regulations/pdf/keito_renkei_20241201.pdf
東京電力パワーグリッド, “系統連系技術要件 託送供給等約款別冊”, 閲覧日:2025年7月14日, https://www.tepco.co.jp/pg/consignment/notification/pdf/keitou_renkei20250131.pdf
サイバーセキュリティ戦略本部, “重要インフラのサイバーセキュリティに係る安全基準等策定指針”, 閲覧日:2025年7月14日, https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf
資源エネルギー庁, “エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver3.0”, 閲覧日:2025年7月14日,
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf 等より三菱総合研究所作成

電力分野の制度・規制等におけるサイバーセキュリティの扱い(2/2)｜ 日本

- 「特定卸供給事業に係るサイバーセキュリティ確保の指針」においては、特定卸供給事業者の届出時に、「サイバーセキュリティ確保の観点から望ましい行為」の内容について実施の詳細を示すことが求められる。
- 「JC-STAR制度」は、2025年3月から★1の運用が開始されている。

特定卸供給事業に係るサイバーセキュリティ確保の指針	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	出力制御機能付PCS等技術仕様	セキュリティ要件適合評価及びラベリング制度(JC-STAR)
アグリゲーターとなる事業者は届出において、以下の内容を示す必要がある。 **【サイバーセキュリティ確保の観点から望ましい行為6項目の主な内容】** ● 経営層の責任を明確化。管理組織を設置。セキュリティ教育の計画・実施と効果の評価 ● セキュリティに関する情報の記録。作成したセキュリティ関連文書の適切な保管・管理 ● 対象システムやネットワーク構成を明確化し、保護すべき情報・機能・資産を特定した上で、対策を策定。適切なセキュリティ対策を選定・実施。適切な報告の仕組みを構築 ● 外部ネットワークとの分離を徹底し、接続点の防御・最小化、通信の認証・暗号化を強化し、データ改ざん対策を実施 ● セキュリティ仕様の明確化とデータ管理の強化。委託先や供給先の対応を適切に管理 ● 情報収集・対応手順の明確化・損害の最小化を重視し、迅速な対応を可能にする体制を構築。関係機関への報告・情報共有・訓練の実施を通じて、事故の予防と再発防止を図る	自家用電気工作物の制御システムのサイバーセキュリティ確保を規定。自家用電気工作物のうち系統連系する発電設備については、他ネットワークとの接続点の最小化、ウイルスチェック等を求めている。 **【対策の概要】** ● 自家用電気工作物のうち系統連系する発電設備において、他ネットワークとの接続点は最小化し、また、他ネットワークとの接続点に防御措置を講じること ● 自家用電気工作物のうち系統連系する発電設備の遠隔監視システムなど制御システム等に接続する外部記憶媒体、および可搬型の機器について、ウイルスチェックを行う	電力系統における発電出力の適切な制御を確保することを目的に規定されており、66kV以上と66kV未満で区分されている(以下は66kV以上の対策の概要)。 **【対策の概要】** ● 一般送配電事業者の電力サーバと発電事業者の通信においては, 専用通信回線を使用 ● 一般送配電事業者、および発電事業者の設備においては「電力制御システムセキュリティガイドライン」に基づきセキリティを管理 ● PCS等監視装置とPCS等間の接続インタフェースのセキュリティについては「電力制御システムセキュリティガイドライン」に基づき管理	2025年3月より運用が開始されたIoT製品のセキュリティを評価し認証ラベルを付与する制度。現時点では、IoT製品共通の最低限の脅威に対応するための基準(★1)の申請・取得が可能。 **【★1で想定する守るべき資産】** ● 有線通信機能・無線通信機能 ● セキュリティ機能 ● 通信機能に関する設定情報 ● セキュリティ機能に関する設定情報 ● 機器の意図する仕様に置いて、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

出所)経済産業省, “特定卸供給事業に係るサイバーセキュリティ確保の指針”, 閲覧日:2025年7月14日,
https://www.enecho.meti.go.jp/category/electricity and gas/electric/summary/regulations/pdf/cyber-shishin.pdf
経済産業省, “自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン”, 閲覧日:2025年7月14日,
https://www.meti.go.jp/policy/safety security/industrial safety/law/files/jikayouguideline.pdf
電気事業連合会他, “出力制御機能付PCSの技術仕様について”, 閲覧日:2025年7月14日, https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/005_02_00.pdf
情報処理推進機構(IPA), “セキュリティ要件適合評価及びラベリング制度(JC-STAR)”, 閲覧日:2025年7月14日, https://www.ipa.go.jp/security/jc-star/index.html 等より三菱総合研究所作成

【参考】ERABガイドラインにおけるJC-STAR制度の扱い

- ERABサイバーセキュリティガイドラインVer3.0においては、リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★1（レベル1）以上を満たす製品であることが求められている。

ERABガイドライン改定箇所の例

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

●全般的な対策

- R6におけるERAB制御対象のエネルギー機器は、リソースアグリゲーターのシステムとインターネット経由で直接通信することから、R5におけるERAB制御対象のエネルギー機器と、R4におけるリソースアグリゲーターの制御対象の機器の２つの特徴を持つ。このため、従来のR5における対策に加えて、R4における対策を併せて実施することが重要。

（①物理的なGWを介さないDRサービスへの対策）

新しく盛り込むべき事項の方向性

3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース）

【勧告】

（インターフェースの対策）

- 外部システムとの相互接続点において、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。
- 管理組織の特定が可能で、かつ脆弱性対策が設計可能であるプロトコルを採用すること。
- リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。
  ※今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たす製品を選択することが望ましい。
- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

出所）資源エネルギー庁, ERABサイバーセキュリティガイドラインの改定状況について, 閲覧日：2025年4月18日,
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/018_06_03.pdf

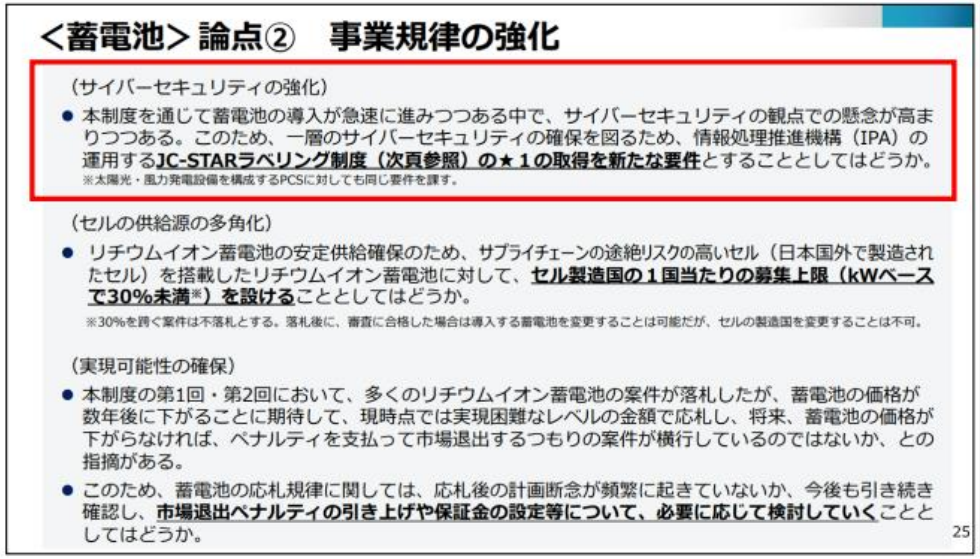
【参考】長期脱炭素電源オークションにおけるJC-STAR制度の扱い

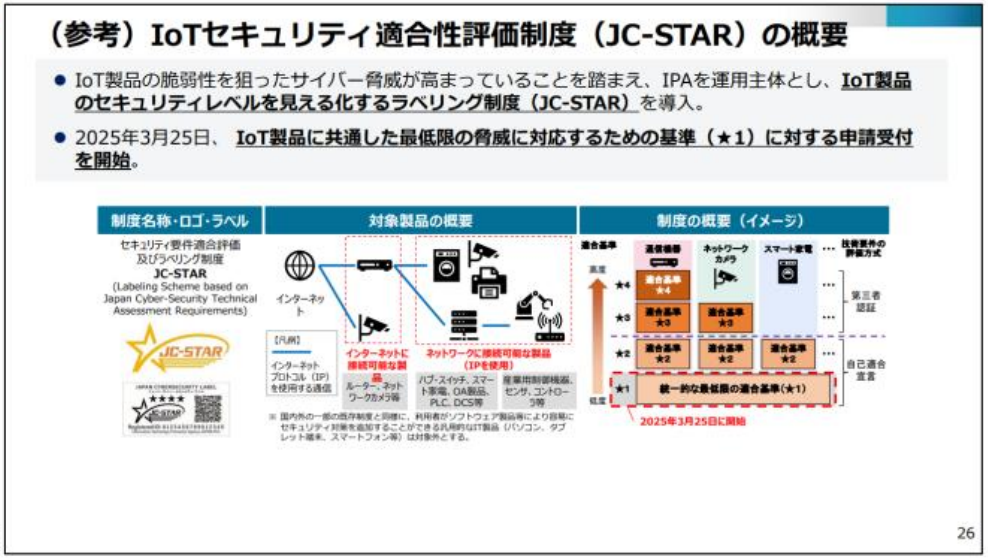
- 第3回長期脱炭素電源オークションにおいて、蓄電池の事業規律強化のため、BMS、PCS、EMS等※について、JC-STAR制度の★1の取得を要件とする方針が示された。

  ※）BMS（バッテリーマネジメントシステム）、PCS（パワーコンディショナー）、EMS（エネルギーマネジメントシステム）等の設備・装置であり、外部と直接通信を行わない場合でも、外部との間接的な通信などを通じて、設備全体に影響を及ぼす可能性のある設備・装置を含む。

- なお、JC-STAR制度では★1のみが申請開始されている状況であり、業界内での検討等により★1セキュリティ要件では十分ではないとされた場合は、IPAと協力して★2以上の基準検討及び制度の整備を行うこととされている。

長期脱炭素電源オークションにおけるJC-STAR制度の扱い





第103回 制度検討作業部会（2025年5月28日）資料３－３を一部修正

出所）資源エネルギー庁, 第104回 次世代電力・ガス事業基盤構築小委員会 制度検討作業部会｜資料3 “長期脱炭素電源オークションについて”, 閲覧日：2025年6月24日, https://www.meti.go.jp/shingikai/enecho/denryoku_gas/jisedai_kiban/system_review/pdf/104_03_00.pdf#page=34

【参考】サイバーセキュリティ関連の制度・規制等 | 米国

- NERC CIPは、系統内のインフラ資産を保護するための法的強制力を持つセキュリティ要件であり、セキュリティ管理やサプライチェーンリスク管理等を定めた13個の文書で構成される。
- DoE（Department of Energy：米国エネルギー省）が実施する支援制度の活用や実証試験を行う場合、事業者はサイバーセキュリティ計画の策定と提出、プロジェクト期間中の定期報告や監査を受ける義務を負う。

NERC CIP

北米系統のサイバーセキュリティリスクや物理的リスクへの対応を規定した13個の文書から構成される。

【13個の文書の項目】

CIP-002	BESサイバーシステム分類
CIP-003	セキュリティ管理コントロール
CIP-004	人的管理と訓練
CIP-005	電子セキュリティ境界
CIP-006	物理的セキュリティ
CIP-007	システムセキュリティ管理
CIP-008	インシデント報告と対応計画
CIP-009	復旧計画
CIP-010	設定変更管理と脆弱性検査
CIP-011	情報保護
CIP-012	通信の保護
CIP-013	サプライチェーンリスク管理
CIP-014	物理的セキュリティの強化

DoE支援制度

DoEが実施する支援制度の活用や実証試験を行う場合、事業者は以下の項目を記載したサイバーセキュリティ計画書の提出が求められる。また、実施期間中は定期的なレビューと監査を受ける必要がある。

【サイバーセキュリティ計画書の内容】

- ネットワーク、システム、デバイス、アプリケーション、コンポーネント間のサイバーセキュリティを維持するための計画
- サイバーセキュリティリスクの継続的な評価と対応策
- ネットワークやシステムへのサイバー攻撃が判明または疑いがあった際の報告
- 脆弱性試験やセキュリティエンジニアリング評価等のDoEが提供するサイバーセキュリティプログラムの活用

Cybersecurity Considerations for DER on the U.S. Electric Grid

分散型エネルギーリソース（DER）の導入拡大に伴う米国電力網におけるサイバーセキュリティに関するレポート（2022年にDoEが発行）。DER全般に適用されるサイバーセキュリティ対策として以下の観点を推奨している。

【推奨されるサイバーセキュリティ対策】

- 設計時からセキュリティを組み込む“Security by design”の導入
- 既存の系統連系要件等の標準やガイドラインを活用したセキュリティ対策の統一
- サプライチェーン全体のセキュリティの強化
- 業界関係者間の情報共有の活性化

UL2941

米国のUL Solutions社とDoE管轄下のNREL（The National Renewable Energy Laboratory）が共同で開発したサイバーセキュリティに関する認証規格。再生可能エネルギーシステムや蓄電システム、EV充電器等の分散型エネルギーリソース（DER）を対象に、アクセス制御や暗号化、遠隔監視におけるセキュリティ要件を定義している。

【要件等の概要】

- 各種DERに対するアクセス制御やユーザー認証、暗号化、遠隔監視セキュリティ、ソフトウェア・ファームウェアの保護等に関する要件が定められている。

出所）FERC, “Cyber and Grid Security”, 閲覧日：2025年7月11日, https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security
OCED, “Cybersecurity Plan Guidance”, 閲覧日：2025年7月11日, https://www.energy.gov/sites/default/files/2023-06/OCED%20Cybersecurity%20Plan%20Guidance.pdf#:~:text=When%20is%20a%20Cybersecurity%20Plan,CESER%20will%20review%20your%20plan
DOE, “Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid”, 閲覧日：2025年7月11日, https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf
UL Solutions, “New Cybersecurity Threats to Renewable Energy Generation”, 閲覧日：2025年7月11日, https://www.ul.com/insights/new-cybersecurity-threats-renewable-energy-generation?utm source 等より三菱総合研究所作成

【参考】サイバーセキュリティ関連の制度・規制等 | EU

- EUのサイバーセキュリティ対策を定めたNIS指令が改正され、2023年1月にNIS2が制定された。インシデント報告の早期義務化等、サイバーセキュリティの執行に関する要件も強化されている。
- また、EUではデジタル要素を有する全ての製品に対してEU Cyber Resilience Act（欧州サイバーレジリエンス法）が適用され、重要度の高い製品については、第三者認証による適合性評価が義務化されている。

NIS 2

EUのサイバーセキュリティ対策を定めたNIS（Network and Information Security： ネットワーク情報セキュリティ）指令を改正したもの。インシデント報告の早期義務化等が要件に含まれる。

【求められる必須対策（第21条に記載）】

a	リスク分析、情報システムセキュリティ方針
b	インシデント対応
c	バックアップや災害復旧、危機管理等の事業継続
d	サプライチェーンセキュリティ
e	ネットワークおよび情報システムの取得、開発、保守におけるセキュリティ
f	サイバーセキュリティリスク管理対策の有効性を評価するための方針および手順
g	基本的なサイバー衛星実践、サイバーセキュリティ研修
h	暗号技術の利用、必要に応じて暗号化に関する方針・手順
i	人的資源のセキュリティ、アクセス制御方針、資産管理
j	多要素認証または継続認証ソリューション、セキュアな音声・映像・テキスト通信、必要に応じた組織内の緊急時セキュア通信システムの利用

EU Cyber Resilience Act

デジタル要素を有する全ての製品に対して適用される。重要度の高い製品（ルーター、通信インターフェース等）に関しては、第三者認証による適合性評価が義務付けられている。

【製造業者（メーカー）の義務】

2027年12月適用開始	必須サイバーセキュリティ要件の充足
	サイバーセキュリティリスク評価の実施・文書化
	対象製品のサイバーセキュリティに関する文書の作成
	脆弱性に対処するための措置の実施
	技術文書の作成
	適合性評価手続の実施
	EU適合宣言書の作成
	対象製品へのCEマークの貼付
	CRAの遵守体制の構築
	対象製品の添付文書等の作成
	ユーザへの対応窓口の設置
2026年9月適用開始	当局への脆弱性・インシデントの報告
	ユーザへの脆弱性・インシデントの通知

network code on cybersecurity for the electricity sector

サイバーセキュリティ担保、リスク評価の標準化、インシデント対応の迅速化等を通じたEU域内の電力供給システムの強化を目的に制定。送配電事業者や発電事業者、電力市場運営事業者に対して以下の勧告的事項を定めている。

【主な要件等】

- 3年ごとのサイバーセキュリティリスク評価の義務化
- インシデント発生時の24時間以内の情報共有義務化
- 技術的保護装置の設置・導入
- サプライチェーン管理　等

出所）European Union, “Document 02022L2555-20221227”, 閲覧日：2025年7月11日, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1747555705208
Cyber Risk GmbH, “Cyber Resilience Act (CRA) | Updates, Compliance,”, 閲覧日：2025年5月20日, https://www.european-cyber-resilience-act.com/
UNITIS, “サイバーレジリエンス法における義務の内容と具体策”, 閲覧日：2025年5月27日, https://unitis.jp/articles/15756/
European Comission, “New network code on cybersecurity for EU electricity sector”, 閲覧日：2025年7月11日, https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en 等より三菱総合研究所作成

【参考】サイバーセキュリティ関連の制度・規制等 | 英国

- NIS regulation 2018は、欧州のNIS指令に対応する国内法として位置付けられる。エネルギー事業者等の基幹サービス事業者は、定期的なレポートをOfgem（Office of Gas and Electricity Markets：ガス・電力市場監督庁）に提出することが求められる。
- また、NIS regulation 2018の更新・強化を目的にCyber Security and Resilience Billの法案内容が審議されている。

NIS regulation 2018

EUのNIS指令に対応する国内法として制定されたものであり、エネルギー事業者は基幹サービス事業者として分類され法の適用対象となる。リスク評価の際には、Cyber Assessment Framework（CAF）に基づいた自己評価の実施が求められる。

【Cyber Assessment Framework（CAF）の項目】

a	セキュリティリスクの管理
b	サイバー攻撃からの防御
c	サイバーセキュリティ事象の検知
d	サイバーセキュリティインシデントの影響最小化
e	非サイバーリスクからの防御（物理的なセキュリティ対策含む）

【基幹サービス事業者に求められるレポート提出】

- 基幹サービス事業者は、定期的なレポート（Annual Report/Check-In Report）をOfgemに提出することが求められる。
- 管理者やシステム構成に関する報告に加え、CAFに基づくリスク評価結果を踏まえた改善計画についてもレポートに含む必要がある。

Cyber Security and Resilience Bill

NIS regulation 2018の更新・強化を目的に、Cyber Security and Resilience Billの法案内容が審議されている。医療・エネルギー分野へのサイバー攻撃増加を受け、EUのNIS2指令よりも厳格な規制が検討されている。

【主な要件等】

- 24時間以内のインシデント報告の義務化
- サプライチェーン管理義務のTier3サプライヤーへの拡大　等

出所）legislation.gov.uk, “https://www.legislation.gov.uk/uksi/2018/506”, 閲覧日：2025年7月11日, https://www.legislation.gov.uk/uksi/2018/506
gov.uk, “Cyber Security and Resilience Bill: policy statement”, 閲覧日：2025年7月11日, https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement 等より三菱総合研究所作成

系統用蓄電システムにおけるサイバーセキュリティ面での現状整理

- 通信機能や遠隔制御等の機能を有するEMSやPCS、BMSは特にサイバー攻撃のリスクを内在しており、これらの設備・機器が適切なサイバーセキュリティ対策を有していることが必要と想定される。
- また、メーカー等もサイバー攻撃の主体となりえる可能性があることを踏まえ、悪意のあるメーカー等の設備・機器を使用しないことも重要であると考えられる。

調査・分析から得られた示唆

	論点	調査・分析結果	得られた示唆
現状・課題	● どの設備・機器がサイバー攻撃の対象となりえるか ● どのようなサイバー攻撃のパターンが考えられるか ● どのようにしてサイバーセキュリティ対策を実施しているか	• EMSやPCS、BMS等のネットワークが接続されている設備・機器は遠隔操作が可能であり、特にサイバー攻撃のリスクがある。 • サイバー攻撃の主体としては、悪意のある第三者または悪意のある事業者（メーカー等）が挙げられる。攻撃経路は通信経由または設備・機器本体が入口となる可能性がある。 • ユーザーはメーカーに仕様を提出し、メーカーは仕様に準じた対策を実施している（空ポートからの物理的な侵入防止等）。	• 系統用蓄電池の事業当事者は、計画段階におけるセキュリティ対策・評価し、運用時の継続的なセキュリティ対策・訓練、インシデント発生時の復旧計画の策定等を適切に講じる必要性が高いと考えられる。
今後の対策	● 蓄電所へのサイバー攻撃により想定されるリスク ● リスクの原因となりうる事象は何か ● 各国の関連規制等ではどのような要件が求められているか	• 蓄電所へのサイバー攻撃により、電力系統・電力品質への影響、事業者の経済損失、蓄電所の火災等のリスクが想定される。 • 上記のようなリスクは、EMSやPCSへのサイバー攻撃による不適切な運転指令やBMSへのサイバー攻撃によるSoC、SoH等のデータ改ざん等が原因として挙げられる。 • 各国のサイバーセキュリティ関連規制等では、インシデント報告やサプライチェーンリスクの管理等を要件としており、文書化や計画提出を求める場合もある。	• EMSやPCS、BMS等は通信機能や遠隔制御等の性質からサイバー攻撃のリスクが内在しており、系統用蓄電池事業においては適切なメーカーから必要十分なセキュリティ機能や安全性を具備した設備・機器を調達することが重要であると考えられる。 • 蓄電所内のネットワーク構成及びセグメンテーション等を整備することで、物理的なサイバーリスクの排除やサイバー攻撃の影響の最小化を図ることが望ましいと考えられる。

未来を問い続け、変革を先駆ける

MRI 三菱総合研究所