２０２３年度
「V2Gビジネスにおけるサイバーセキュリティに関する動向調査」に係る公募説明資料

2023年5月29日

NEDO　スマートコミュニティ・エネルギーシステム部

概要

【背景・目的】

- 国内外では、カーボンニュートラルに対する取り組みが活発化しており、今後、更に再生可能エネルギーを大量導入していくために、欧米や豪州等においては、高度なデジタル技術を活用し、多数の 分散型エネルギーリソース（DER：Distributed Energy Resources）を遠隔・統合制御することで、負荷平準化や再生可能エネルギーの供給過剰の吸収等（DER フレキシビリティ）による系統混雑の解消に取り組んでおり、今後はEVも負荷として考えるだけでなく、系統安定化のためのリソースとして活用する動き（V2G：Vehicle to Grid）が活発化すると見込まれている。
- こうした流れを受け、国内でも資源エネルギー庁の「次世代の分散型電力システムに関する検討会」において、V2Gビジネス構築に向けた検討が開始され、今後はビジネス構築に対する検証のため国際実証の展開が予想される。V2Gでは、EVを発電機や蓄電池のようにリソースとして取り扱うことが多いため、電力系統向けのサイバーセキュリティが重要となってくるが、現状では、V2Gで使用する通信プロトコルや自動車会社に対するサイバーセキュリティ要件は定められつつあるものの、充電器に対するセキュリティ基準が検討されていない状況である。
- 本調査ではV2Gビジネスの海外実証実施に向けたポテンシャル調査などの検討に寄与すべき情報を得ることを目的として、国内外におけるV2Gに関する実証などの取り組み状況を調査するとともに、その中でサイバーセキュリティについてどのような対応をしているかを調査する。あわせて、EV以外のDERを電力系統に接続する際のサイバーセキュリティの動向についても調査し、充電器に対するサイバーセキュリティの考え方について整理するとともに、EVユーザーに対するプライバシー保護の考え方について整理する。

【事業期間】

- 2023年度（１年間）

【事業規模】

- 20百万円以内

調査内容（国内外動向調査）
（仕様書3.(1)(2)項）

海外（特に欧米）、及び国内におけるV2Gビジネスにおけるサイバーセキュリティへの取り組み状況について、以下の項目に重点を置いて調査する

①セキュリティ上における脅威はどのようなものを想定しているか
（外的アタッカーなど）

②ユーザー側のリスクはどのようなものを想定しているか

③その対策はどうなっているか
- 個別機器での対応
- システムでの対応
- 制度（ルール）での対応
- 組織、マネジメントでの対応

④標準化への取り組みはどうなっているか

⑤他の分散電源に対する取り組みとの違いはあるか

⑥個人情報保護（プライバシー保護）の観点での取り組みはどうなっているか

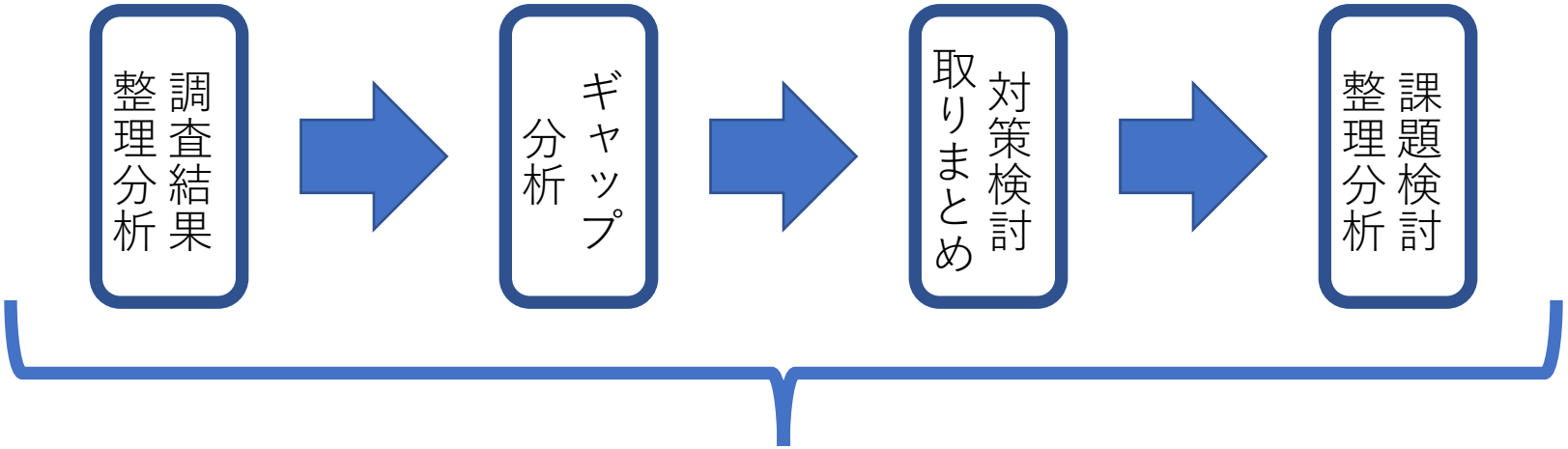
参考（国内外動向調査整理案）

比較表

項目		海外（欧米）			国内
		A国	B国	C国	
想定事項	脅威				
	ユーザリスク				
対策	個別機器				
	システム				
	制度（ルール）				
	組織、マネジメント				
標準化への取り組み					
他の分散電源に対する取り組みとの違い					
個人情報保護（プライバシー保護）の取り組み					

調査内容（まとめ）
（仕様書3.(3)項）

（１）、（２）項の調査により得られた結果を整理分析し、海外と我が国の取り組みについてギャップ分析を行うとともに、今後、我が国がとるべき対策をまとめ、対策を進めるうえでの課題等についても分析整理する。
また、V2Gを実現する上でのサイバーセキュリティやプライバシー保護において、標準化すべき課題についても整理する。
その上で、それらの課題解決に向けた実証を想定した場合のユースケースとしてまとめる。



- **標準化すべき課題整理**
- **課題解決を目的とした実証のユースケース提案**

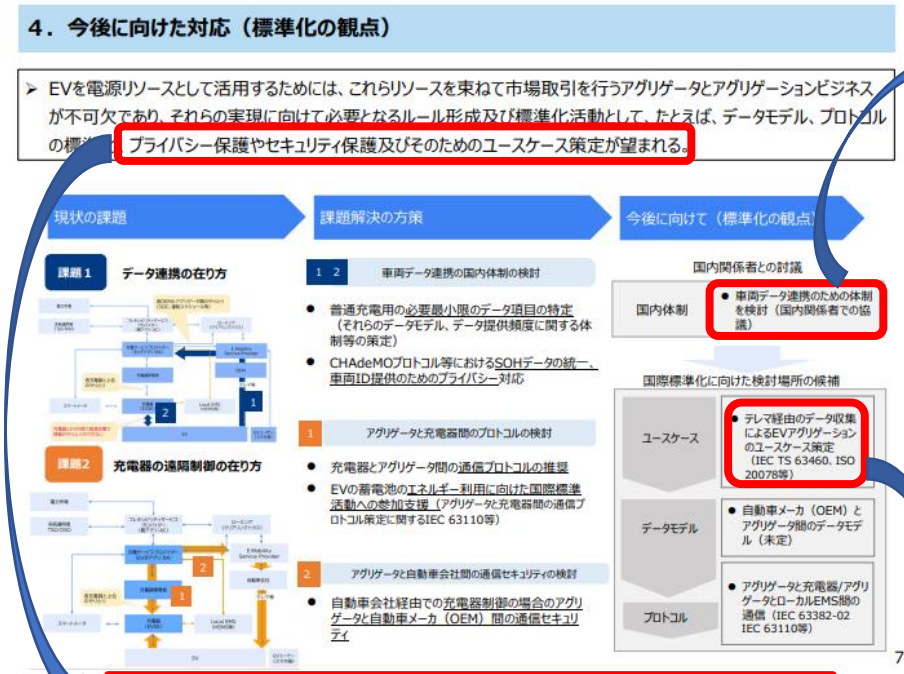
進め方
（仕様書3.(4)項）

- 文献調査やNEDO職員及び国内有識者とともに**国内外ヒアリング**を行う等の方法により得られた情報について、国内有識者・専門家との意見交換等を実施して情報共有しながら事業を実施する。
- 調査対象分野に係る有望な技術の内外優位性、脅威などを分析し、**国内で実装する上での技術的課題、経済的課題（コスト）、インフラ上の課題、制度（規制等）上の課題**などを整理する。また、課題を克服し、該当分野において我が国の国際競争力を確保出来る複数のシナリオを提示する。
- ヒアリング先および内容については、NEDOと調整の上、**経済産業省**、関連の事業者や業界団体等を含め、広く知見を持つ専門家からの意見を聴取する。
- 調査した各テーマについて、成果報告書とは別に、テーマの概要を図示した資料を**テーマごとにパワーポイント5枚程度ずつ作成**する。

参考（国内の動き）

第4回スマート・システム標準専門委員会

資料４「電動車（EV）を活用した電力アグリゲーションビジネスにおけるユースケースの標準化に向けた課題の整理」　7ページ



プライバシー保護や**セキュリティ保護**及びそのための**ユースケース策定**が望まれる

テレマ経由のデータ収集によるEVアグリゲーションのユースケース策定

第5回 次世代の分散型電力システムに関する検討会

資料4「EV等の電力システムにおける活用に関する今後の検討方針について」　20ページ

車両データ連携のための体制を検討（国内関係者での協議）

EVグリッドワーキンググループ（仮称）の立ち上げについて

- **様々なステークホルダーにとって望ましいEVと電力システムとの統合の実現に向けて、関係業界が互いの課題を解決しあえる仕組みを、業界の垣根を越えて検討し、足元から必要な対策を着実に講じていくべく、来年度、EVグリッドワーキンググループ(仮称)を立ち上げることとしたい。**
- 検討にあたっては、下記の検討体制とし、**来年度内を目途に、データ取得等のルール検討をはじめ、諸課題に対して講ずるべき施策等を検討し、本検討会に報告することとしたい。**

検討体制（案）

- 自動車メーカー
- 充放電器等機器メーカー
- 充電器サービサー
- 一般送配電事業者
- 小売電気事業者
- アグリゲーター
- データプラットフォーマー
- 有識者（標準有識者含む）

<事務局>
- 資源エネルギー庁　電力・ガス事業部、省エネルギー・新エネルギー部
- 製造産業局　自動車課
- 産業技術環境局　国際電気標準課

来年度内を目途に、**データ取得等のルール検討**をはじめ、諸課題に対して講ずるべき施策等を検討し、本検討会に報告することとしたい。

参考（本調査の活用目標）

本調査

- 標準化すべき課題整理
- 課題解決を目的とした実証のユースケース提案

海外実証ポテンシャル調査
（NEDO事業を想定）

V2Gにおける「プライバシー保護」、「サイバーセキュリティ」に関する標準化について検討するためのユースケースを整理し、実証可能な地域を検討する。

NP提案委員会
（設置に向けた事前調整・議論の場も含む）

ポテンシャル調査にて策定したユースケースに基づきNP提案を作成。
海外実証で得られた知見も活用し提案する。

連携

海外（国内）実証
（NEDO事業を想定）

ポテンシャル調査にて選定した地域でV2G実証を行う。

参考資料

V2G ビジネスにおけるサイバーセキュリティに関する動向調査 結果概要

※2022年度に実施したNEDO調査事業「スマートコミュニティ関連技術やサービスに関する標準化及び海外動向調査」より

調査概要

【概要】

国内外の電力系統におけるサイバーセキュリティガイドラインについて調査整理し、V2G特有の要件と考えられる項目（ターゲット）における課題について整理した。

① 調査対象国内ガイドライン
- 電力制御システムセキュリティガイドライン
- 系統連系技術要件
- 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
- ERABに関するサイバーセキュリティ ガイドライン Ver2.0

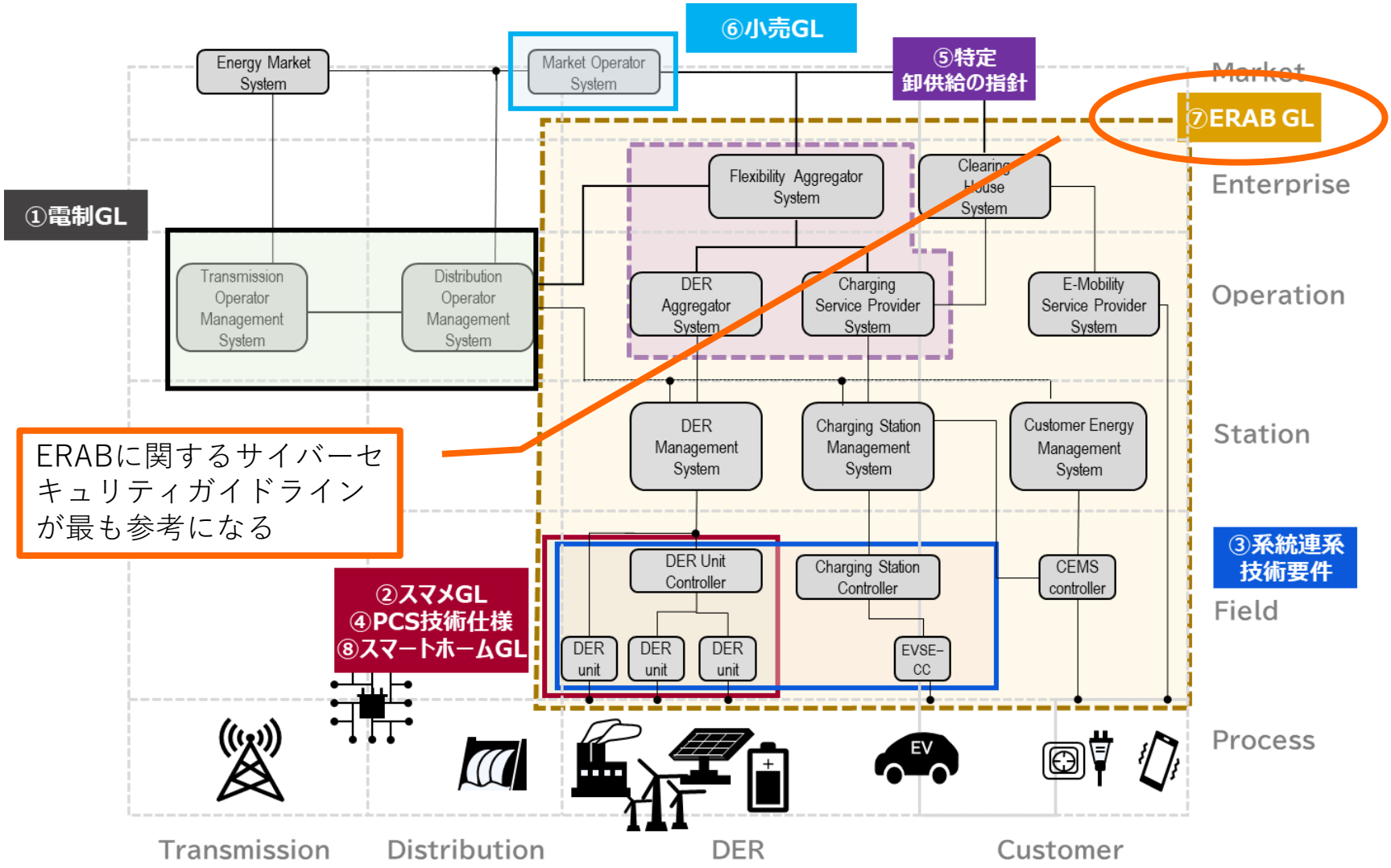
② 調査対象海外ガイドライン
- NERC Critical Infrastructure Protection Standard（CIP基準）
- NIS（Network and Information Systems）2指令

③ ターゲット
- V2Gにおける通信規格要件
- 充電器・EV・自動車会社（OEM）のセキュリティ基準

【結論】

ERABに関するサイバーセキュリティガイドラインを基に必要な課題を検討した結果、OEMに対するセキュリティ基準は、国際的に法制化されており、通信規格においても一部を除きセキュリティに関する検討が進み、更新版においてセキュリティ要件が厳格化されているもの、充電器に対するセキュリティ基準は現状検討できていないことがわかった。

国内のガイドライン等とSmart Grid Architecture Model（SGAM）の整理



国内のガイドラインの概要まとめ

	名称	主な対象	位置づけ	発行主体	概要
①	電力制御システムセキュリティガイドライン	電気事業の用に供する電気工作物	義務	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。
②	スマートメーターシステムセキュリティガイドライン	スマートメーターシステム	義務	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。
③	系統連系技術要件	系統連系する発電設備	義務	経済産業省	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。
④	出力制御機能付PCSの技術仕様	出力制御機能付PCS	義務	各一般送配電事業者	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。

電力制御システムセキュリティガイドラインの対策要件

組織的対策
- 経営層の責任
- セキュリティ管理組織の設置
- 役割の定義
- 委託先の管理
- 教育の実施
- 文書の管理
- セキュリティマネジメントシステムの構築
- セキュリティインシデントへの対応
- 訓練の実施

技術的対策
- ネットワークの分離
- 他ネットワーク接続点の最小化
- 通信データの保護
- 機器のマルウェア対策
- 不正処理の防止
- アクセス制御
- ログの取得
- セキュリティ仕様の確認
- データ管理
- 外部媒体のマルウェア対策
- 管理者権限の割当
- セキュリティパッチの適用
- 入退管理

系統連系技術要件で求められる3つの対策の概要

観点	求められる対策
サイバーインシデントの発生を防ぐ事前防御	対策① ネットワーク接続点の保護
	対策② データの保存・転送を行う機器・端末等のマルウェア対策
インシデント発生時の影響を最小化する事後対応（早期発見、迅速な対処）	対策③ 連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知

国内のガイドラインの概要まとめ

	名称	主な対象	位置づけ	発行主体	概要
⑤	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	アグリゲーター	義務	経済産業省	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ある。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。
⑥	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	小売電気事業者	任意	経済産業省	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。
⑦	ERABに関するサイバーセキュリティ ガイドライン Ver2.0	ERABに関する事業者	任意	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。
⑧	スマートホームの安心・安全に向けた サイバー・フィジカル・セキュリティ対策ガイドライン	住宅事業者・IoT機器ベンダーなどのスマートホームに関わるステークホルダー	任意	経済産業省	スマートホームの提供事業者をはじめスマートホームの住まい手 など幅広い関係者に、スマートホームにおける安心で安全な暮らしを実現するための セキュリティに関する基本的な指針を示したガイドライン。

特定卸供給に係るサイバーセキュリティ確保の指針における対策要求事項

組織
- 体制（経営層の責任等）
- 役割（責任者の任命、委託先管理等）
- セキュリティ教育

文書化
- 文書管理、実施状況の報告

セキュリティ管理
- セキュリティ管理（セキュリティマネジメントシステムの構築）

設備・システムのセキュリティ
- 外部ネットワークとの分離
- 他ネットワークとの接続（接続点の最小化、防御等）
- 通信のセキュリティ（暗号化、通信プロトコル等）
- 機器のマルウェア対策
- アクセス制御（接続制御、通信相手の認証等）

運用・管理のセキュリティ
- 外部記憶媒体等のマルウェア対策

セキュリティ事故の対応
- 情報の収集（セキュリティ事故対応に必要な情報の収集）
- セキュリティ事故の対応（対応体制、手順の明確化等）
- セキュリティ事故の報告と情報共有
- 周知と訓練（訓練の定期的実施　等）

赤字：「電力制御システムセキュリティガイドライン」の勧告事項
青字：「ERABに関するサイバーセキュリティガイドライン Ver2.0」の勧告事項

海外のガイドライン概要

NERC Critical Infrastructure Protection Standard（CIP基準）

- 実装が望まれる対策・実施状況測定の明確さを高めるために、具体性の高い基準が記載されている。
- 基準に従わない場合は、厳しい罰則が示されており、実例も存在する。

CIP基準におけるセキュリティ対策要件

組織的対策

- セキュリティマネジメントの管理（CIP-003-8）
- 人的セキュリティと訓練の実施（CIP-004-6）
- インシデント対応計画（CIP-008-5）
- 電力設備の復旧計画（CIP-009-6）
- サプライチェーンリスク管理（CIP-013-1）

技術的対策

- 電気的セキュリティ境界の保護（CIP-005-5）
- 電力設備の物理セキュリティ（CIP-006-6）
- システムセキュリティ管理（CIP-007-6）
- 設定変更の管理と脆弱性の特定（CIP-010-2）
- 情報の保護（CIP-011-2）
- コントロールセンター間の通信（CIP-012-1）※
- 物理セキュリティ（CIP-014-2）

NIS（Network and Information Systems）2指令

- NIS2指令は、EU全体のサイバーセキュリティ方針であり、詳細な対策要件は規定されていない。具体的な対策要件や対象となる事業者の区分は各国監督省庁の裁量によって決められていく予定である。

３つの目標とNIS2で提案された具体案

セキュリティリスクの管理

- インシデント対応・危機管理、脆弱性の取扱・開示、セキュリティテスト、暗号化の利用などについてのセキュリティ要求事項の強化
- セキュリティリスク管理措置の遵守について、企業経営者への説明責任の要求　など

協力関係の強化

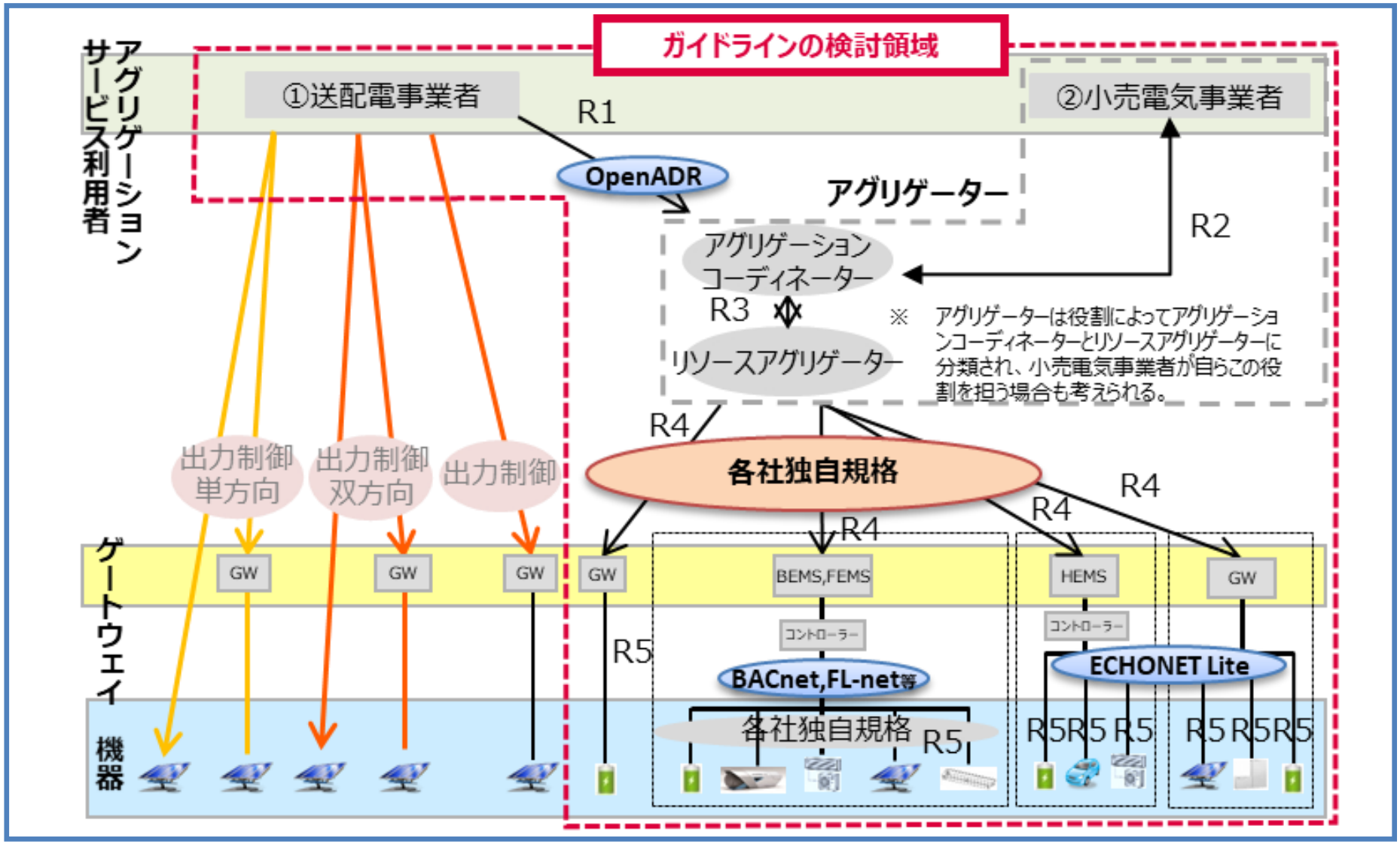
- EUレベルでの大規模なセキュリティインシデントに対する処置を支援するEUサイバー危機連絡組織ネットワーク（EU-CyCLONe）の創設
- 新たに発見された脆弱性に対して、EU全域で連携した脆弱性情報の共有　など

セキュリティ能力の向上

- 各主体がセキュリティ対策を講じるような、より厳格な監督手段と法執行措置の導入
- セキュリティリスク管理および報告義務の侵害に対する制裁金などの行政処分一覧表の策定　など

ターゲットにおける課題抽出
（ERABに関するサイバー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の想定図



出所）ERABに関するサイバーセキュリティガイドライン Ver2.0

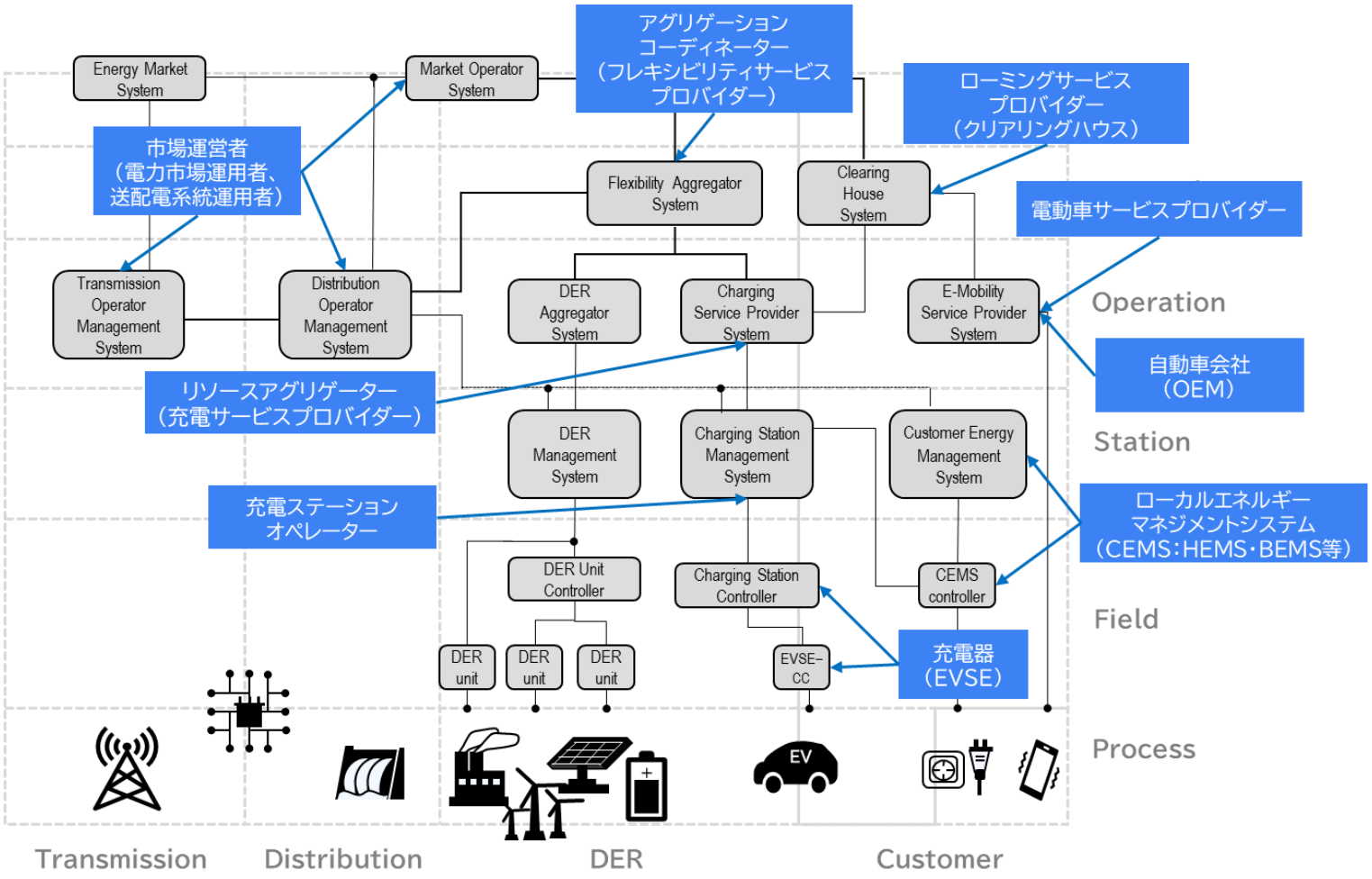
ターゲットにおける課題抽出
（ERABに関するサイバーセキュリティガイドライン）

ERABに関するサイバーセキュリティガイドラインにおけるR1～R5の定義と対策

インターフェース	対象	対策
R1	簡易指令システムとアグリゲーションコーディネーター（AC）間	• 簡易指令システムとの直接的な接続部は、送配電事業者のセキュリティ要求事項に準拠すること • 不特定多数がアクセスできるネットワークと原則分離すること • 他ネットワークとの接続点は最小化し、接続点に防御措置を講じること • 外部システムとの系統連系点において認証すること • 通信メッセージは認証・暗号化により保護すること • ACはRAのサービス品質の責任を持つこと • 電制ガイドラインに基づきセキュリティ要求事項に準拠すること
R2	小売電気事業者とアグリゲーションコーディネーターまたはリソースアグリゲーター（RA）間	• 外部システムとの系統連系点において認証すること • 通信メッセージは認証・暗号化により保護すること • 小売電気事業者はアグリゲーターが求めるセキュリティ要件に準拠すること（基本はERABに関するサイバーセキュリティガイドラインに従うこと）
R3	アグリゲーションコーディネーターとリソースアグリゲーターの間	• 外部システムとの系統連系点において認証すること • 通信メッセージは認証・暗号化により保護すること • RAはACが求めるセキュリティ要件に従うこと（基本はERABに関するサイバーセキュリティガイドラインに従うこと）
R4	リソースアグリゲーターとGWまたはBEMS・HEMS 等エネルギーマネジメントシステム間	• 外部システムとの系統連系点において認証すること • 通信メッセージは認証・暗号化により保護すること • GWやエネルギーマネジメントシステムはACが求めるセキュリティ要件に従うこと（基本はERABに関するサイバーセキュリティガイドラインに従うこと）
R5	需要家側に設置されるERAB制御対象のエネルギー機器間のインターフェース	• 通信メッセージは認証・暗号化により保護すること • ガイドラインを基にIoTに関するセキュリティ対策を実施すること

ターゲットにおける課題抽出
（EVと電力系統のやり取りに注目した整理）

チャージャーセントリック方式・OEMセントリック方式とSGAMの対応



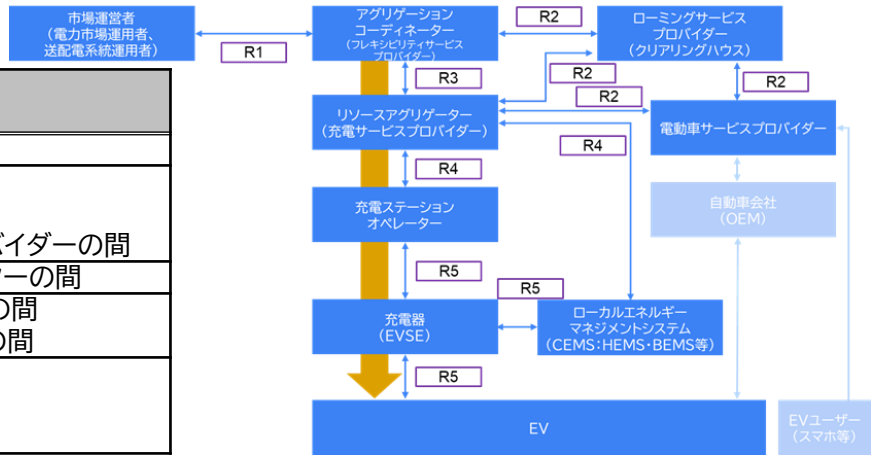
ターゲットにおける課題抽出
（EVと電力系統のやり取りに注目した整理）

「チャージャーセントリック」方式

構成要素の対応関係

インターフェース	対象
R1	市場運営者とアグリゲーションコーディネーターの間
R2	アグリゲーターとローミングサービスプロバイダーの間 アグリゲーターと電動車サービスプロバイダーの間 ローミングサービスプロバイダーと電動車サービスプロバイダーの間
R3	アグリゲーションコーディネーターとリソースアグリゲーターの間
R4	リソースアグリゲーターと充電ステーションオペレーターの間 リソースアグリゲーターとローカルマネジメントシステムの間
R5	充電ステーションオペレーターと充電器の間 ローカルエネルギーマジ面とシステムと充電器の間 充電器とEVの間

概要図

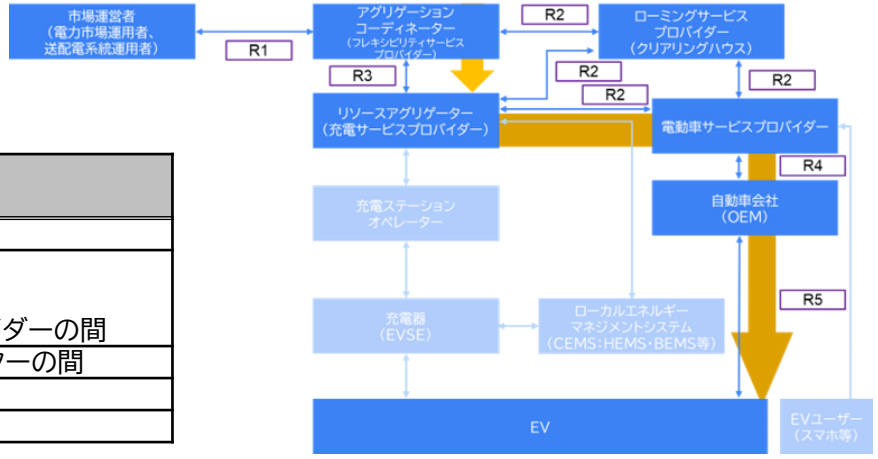


「OEMセントリック」方式

構成要素の対応関係

インターフェース	対象
R1	市場運営者とアグリゲーションコーディネーターの間
R2	アグリゲーターとローミングサービスプロバイダーの間 アグリゲーターと電動車サービスプロバイダーの間 ローミングサービスプロバイダーと電動車サービスロバイダーの間
R3	アグリゲーションコーディネーターとリソースアグリゲーターの間
R4	リソースアグリゲーターと自動車会社（OEM）の間
R5	自動車会社（OEM）とEVの間

概要図



ターゲットにおける課題抽出（ERABに関するサイバー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で検討されている分散電源の脅威に対するV2Gにおける想定脅威

ERABに関するサイバーセキュリティガイドラインにおける脅威	V2Gにおける想定脅威
攻撃者がネットワークを介してGW を超えて、BEMS・HEMSコントローラ、エンドポイントに位置する機器やセンサに不正データを送信し、誤作動、機能を停止、データ取得を不可能にさせる。	アグリゲーター（アグリゲーションコーディネータ・リソースアグリゲーター）、サービスプロバイダー（ローミングサービスプロバイダー、電動車サービスプロバイダー）のネットワークに攻撃者が侵入し、ローカルマネジメントシステムや充電器、EV自身に不正データを送信し、誤作動、機能を停止、データ取得を不可能にさせる。
エンドポイントに位置するエネルギー機器やセンサの内部データ改ざんや盗難が発生する。	ローカルマネジメントシステムや充電器やEVに侵入され、内部データ改ざんや盗難が発生。
エネルギー機器やセンサの不正改造により、誤作動、機能を停止させる。	充電器やEVの不正改造により、誤作動、機能を停止させる。
乗っ取ったセンサやエネルギー機器からERAB システムを構成するサーバーへのデータ送信により処理負荷を増加させ、その結果としてERAB サービス全体を停止させる。	EVや充電器が乗っ取られ、ERAB システムを構成するサーバーへのデータ送信により、処理負荷を増加させ、その結果としてERAB サービス全体を停止させる。
攻撃者がエネルギー機器やセンサを乗っ取り、GW 経由の外部システムへのDoS 攻撃へ加担させる。	攻撃者が充電器やEVを乗っ取り、GW 経由して無関係のシステムへのDoS 攻撃へ加担させる。
設備の破壊や停止の結果として、ERAB サービスの停止、人命に関わる動作が誘発される。	充電器やEVなどの破壊や停止の結果として、ERAB サービスの停止、人命に関わる動作が誘発される。

ターゲットにおける課題抽出
（V2Gにおける通信規格要件）

V2Gにおける通信規格

No	通信規格名	対象通信区画	セキュリティ要件	認証プログラムの有無
1	IEC 63110	• リソースアグリゲーター ⇔ 充電ステーションオペレーター • 充電ステーションオペレーター ⇔ 充電器	○	×
2	OCPP (Open Charge Point Protocol)	• 充電ステーションオペレーター ⇔ 充電器	○	○
3	IEC 61851	• 充電器 ⇔ EV	×	○
4	ISO 15118	• 充電器 ⇔ EV	○	×

IEC 61851 以外はセキュリティに関する検討が進んでおり、更新版において<u>セキュリティ要件が厳格化</u>されている。

ターゲットにおける課題抽出
（充電器・EV・自動車会社のセキュリティ基準）

セキュリティ基準

No	通信規格名	義務・推奨	対象	概要
1	WP-29 UN-R155（ISO/SAE21434）	義務	自動車会社（OEM）	• 車両のサイバーセキュリティおよびサイバーセキュリティ管理システム（CSMS）を定めた国連のサイバーセキュリティ法規 • UN-R155がCSMSの構築する上で参照としているISO/SAE 21434では、車両のライフサイクルにおけるセキュリティ対策について記載されている
2	WP-29 UN-R156	義務	自動車会社（OEM）	• 車両のソフトウェアアップデートを定めた国連のサイバーセキュリティ法規
3	自動車産業サイバーセキュリティガイドライン	推奨	自動車会社（OEM）	• 日本自動車工業会と日本自動車部品工業会が共同で、自動車産業のサイバーセキュリティ対策の向上と点検を目的に作成したセキュリティガイドライン • 最低限・標準・目指すべき目標の3つのセキュリティレベルが設定され、セキュリティレベルごとに満たすべき要件が定義されている

充電器を対象としたセキュリティ基準・ガイドラインを確認することはできなかった。

ターゲットにおける課題抽出
（充電器・EV・自動車会社のセキュリティ基準）（参考）

ISO/SAE21434の要件

要件
組織サイバーセキュリティ管理（Organizational Cybersecurity Management）
プロジェクト依存のサイバーセキュリティ管理（Project Dependent Cybersecurity Management）
分散型のサイバーセキュリティ活動（Distributed Cybersecurity Activities）
継続的サイバーセキュリティ活動（Continual Cybersecurity Activities）
コンセプト（Concept）
製品開発（Product Development）
サイバーセキュリティ妥当性確認（Cybersecurity Validation）
製造（Production）
運用とメンテナンス（Operations and maintenance）
サイバーセキュリティ・サポートの終了と破棄（End of cybersecurity support and decommissioning）
脅威分析とリスクアセスメント法Threat analysis and risk assessment methods

自動車産業サイバーセキュリティガイドラインの要件

カテゴリ	要件
共通	1方針
	2機密情報を扱うルール
	3法令順守
	4体制(平時)
	5体制(事故時)
	6事故時の手順
	7日常の教育
守る対象を明確にし、リスクを特定する（特定）	8他社との情報セキュリティ要件
	9アクセス権
	10情報資産の管理(情報)
	11情報資産の管理(機器)
	12リスク対応
	13取引内容・手段の把握
	14外部への接続状況の把握
	15社内接続ルール
攻撃を防ぐ対策実施(防御)	16物理セキュリティ
	17通信制御
	18認証・認可
	19パッチやアップデート適用
	20データ保護
	21オフィスツール関連
攻撃されたことを迅速に知るために(検知)	22マルウェア対策
	23不正アクセスの検知
検知被害の対応と修復(対応・復旧)	24バックアップ・復元(リストア)