経済産業省

資料４

サプライチェーン・リスクへの対策に関する手引き文書の作成について

2024年10月22日

資源エネルギー庁　電力産業・市場室

サプライチェーン・リスクへの対策に関する手引き文書の必要性について

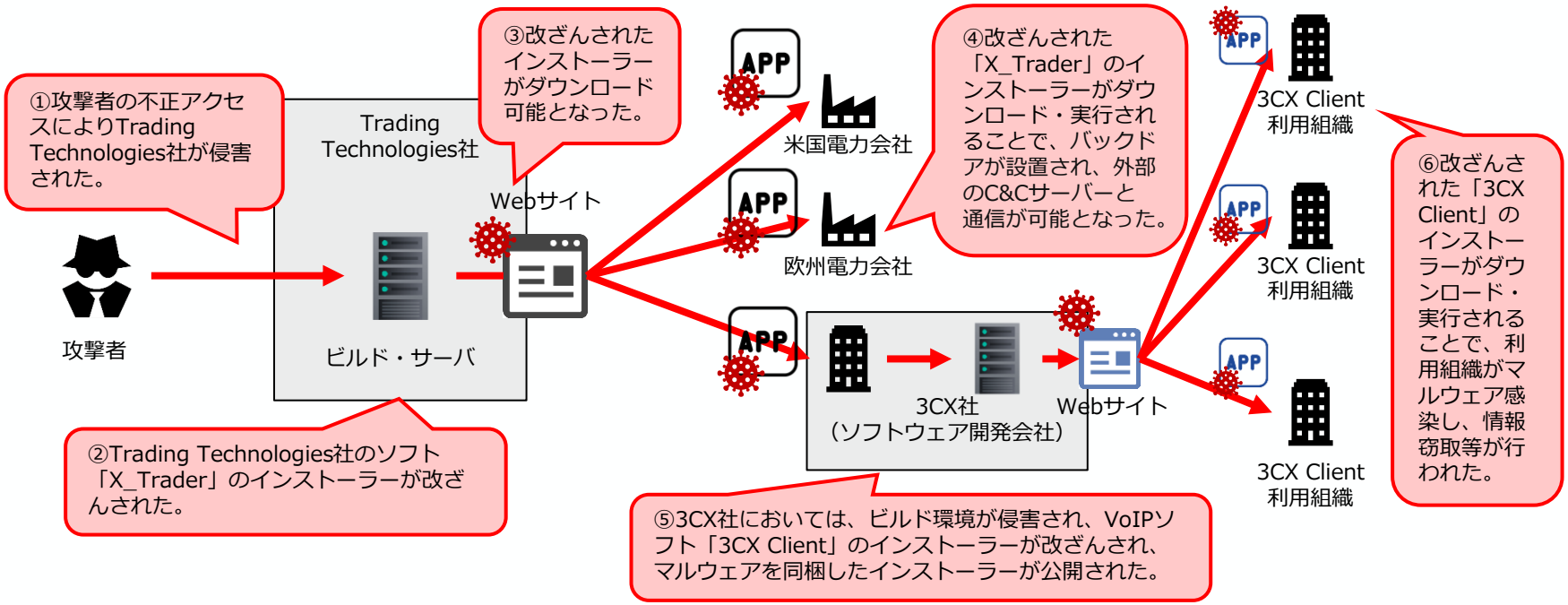
- 電力分野に限らず、重要インフラ全体でサプライチェーン・リスクが高まりつつある。
- このリスクに対処するため、令和5年に策定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」では、重要インフラ分野に共通して求められる取組としてサプライチェーン・リスクに関する対応が明記されたほか、経済安全保障推進法に基づく取組も進んでいる。
- 電力分野における取組として、昨年度の電力SWGの議論を踏まえ、「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」を公表した。今後、この提言内容を踏まえ、「電力制御システムセキュリティガイドライン」の見直しが行われる予定であり、サプライチェーン・リスクへの対応の事項が追加される見込みである。
- 一方で、「電力制御システムセキュリティガイドライン」に記載されるのは、対応の要求事項であり、具体的な対策については、各事業者が検討し、実施していくことになる。
- 中小規模の事業者をはじめとして、多くの事業者がサプライチェーン・リスクに対する対策に課題を抱えているところ、事業者の対応を促進するためには、具体的な対策手順等を整理することが有効ではないかと考えられる。
- これらの状況に鑑み、サプライチェーン・リスクに対する事業者の対応を促進するための具体的な対策手順等を示した手引き文書を作成したい。

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

(1) 先物取引ソフトを通じたサイバー攻撃

- 2023年3月、Trading Technologies社が提供する**先物取引ソフト「X_Trader」の正規インストーラーが改ざん**され、当該ソフトを利用する**電力会社やソフトウェア開発会社にサイバー攻撃が実施**された。
- 3CX社においては、同社の**VoIPソフト「3CX Client」のビルド環境が攻撃の影響**を受け、**同製品のインストーラーにマルウェアが同梱**された。この結果、**3CX Clientの利用組織にも影響が波及**し、**当該利用組織におけるマルウェア感染や情報漏えい等が発生**。

先物取引ソフトウェア（X_Trader）に関連する一連のサプライチェーンセキュリティ攻撃のイメージ



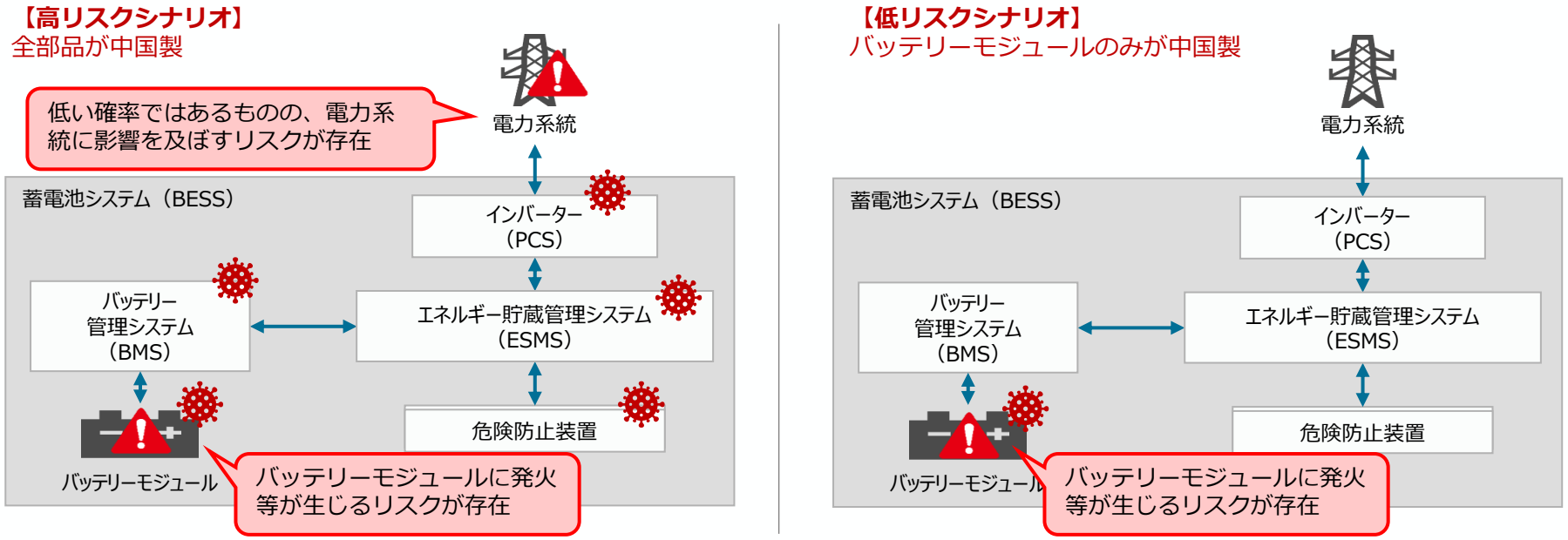
出所）公開情報に基づき三菱総合研究所作成
https://symantec-enterprise-blogs.security.com/blogs/japanese/xtradernosafuraichiengongjimiguoyayorotsuhanozhongyaoinfurazuzhiniyingxiang
https://thehackernews.com/2023/04/lazarus-xtrader-hack-impacts-critical.html

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

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

(3) 米国商務省による中露のコネクテッドカーの輸入・販売を禁止する規則案

- 2024年9月、米国商務省は、**中国とロシアの企業等によって製造・開発された技術※1を用いたコネクテッドカーの輸入や販売を禁止する規則策定案公告（NPRM） を発表**した。
- 商務省長官は、本規則案の背景として、外国の敵対者が、**運転手・同乗者等の大量の機密データを収集・記録するおそれ**があること、**コネクテッドカーを遠隔操作・遠隔無効化するおそれ**があることを挙げている。
- また、中国を対象とした理由として、**国家安全保障上の脅威や中国政府の介入状況**を挙げている。
- 商務省は、10月29日まで、本規則案についてのパブリックコメントを実施している。

※1：中露の企業などによって製造・開発された車両接続システム（テレマティクス制御ユニット、Bluetooth、セルラー、衛星通信、Wi-Fiモジュールなど車両が外部との通信を可能にする一連のシステム）と自動運転システム（運転手なしで車両を自律的に運転できるようにするためのシステム）が対象となる。中露の所有、支配下にある、又は司法権が及ぶ、或いはこれらの国からの指示に従う者によって設計、開発、製造、供給される場合も対象となる。

規則案策定の背景

コネクテッドカーに対する外国敵対者による脅威	中国を対象とした理由
① 運転手や同乗者の大量の機密データを収集し、カメラやセンサーを定期的に使用して米国のインフラの詳細な情報を記録するおそれがある	① 中国の自動車セクターにおける国家統制の規模は、コネクテッドカーに関連する国家安全保障上の脅威を増大させていること
② コネクテッドカーと直接やり取りし、遠隔操作や遠隔無効化をするおそれがある	② 中国政府と自動車セクターとの軍事的結びつきが現在でも存在する
	③ 軍民融合に限らず、中国企業に対する中国政府の介入が増大しており、中国企業が有するコネクテッドカー関連の情報を中国政府が法的に入手できる状況にある
	④ 中国共産党は高いサイバー攻撃能力を有するため、コネクテッドカーに対する攻撃により、社会的混乱を誘発するほか、米軍の行動を制限するおそれもある

出所）DoC BSI, Commerce Announces Proposed Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign, JETRO, 米商務省、中国とロシアが関係するコネクテッドカーの輸入または販売を禁止する規則案を発表 https://www.jetro.go.jp/biznews/2024/09/e98d16fbe974eee6.html に基づき三菱総合研究所作成

電力制御システムのサプライチェーン・セキュリティ向上策に関する提言

- サプライチェーン・リスクが増大している状況を鑑み、前回の電力SWGにおいて、**電力制御システムのサプライチェーン・セキュリティ向上策**について議論を行った。
- 2024年3年、電力SWGの議論結果を提言として取りまとめ、公開した。
- 文書では、**電力制御システムの代表的なサプライチェーン・リスクに対し、事業者に求められる取組を整理**しているほか、**政府が対応を進めていくべき事項を提言**している。
- 本提言内容を踏まえ、**今後、「電力制御システムセキュリティガイドライン」の見直しが行われる予定**である。

電力制御システムのサプライチェーン・セキュリティ向上策に関する提言（2024年3月）


電力制御システムのサプライチェーン・セキュリティ向上策に関する提言

令和６年３月２３日
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

はじめに

我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、平成29年12月に「産業サイバーセキュリティ研究会」が設置され、制度・技術・標準化を検討するワーキンググループ１では、産業分野ごとのサブワーキンググループを設置した。

重要インフラにも電力分野においてサイバーセキュリティ対策強化に向けたさらなる取組が求められているところ、電力分野のサイバーセキュリティに関する今後の取組について検討を行うため、電力サブワーキンググループ（以下、「電力SWG」という。）を平成30年８月に設置し、これまで16回の会合を開催してきた。平成30年11月には、第２回電力SWGまでの議論を取りまとめた提言である「電力制御システムのセキュリティ向上策に関する提言」を発表したほか、以降の電力SWGでは、大手電力事業者、小売電気事業者、小規模発電設備等に求められるサイバーセキュリティ確保の方策に関する議論や電力分野におけるサイバーセキュリティリスク点検ツールに関する議論を行ってきた。

重要インフラ全体の取組としては、「重要インフラのサイバーセキュリティに係る行動計画」（以下、「行動計画」という。）が令和４年６月に策定され、官民連携による重要インフラ防護の一層の強化が進められている。また、行動計画に基づき、重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を整理した「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」（以下、安全基準等策定指針という。）及び安全基準等策定指針でのサイバーセキュリティ確保に向けた取組についての参考情報を記載した「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」が令和５年７月に策定された。安全基準等策定指針では、リスクマネジメントによる事前対応と、危機管理の両面からサイバーセキュリティの確保に取り組むことの重要性が明記されており、具体的なリスクマネジメントの一つとして、サプライチェーン・リスクに対するサプライチェーン・リスクマネジメントを求めている。

本資料は、安全基準等策定指針の策定を踏まえ、電力制御システムのサプライチェーン・リスクに対するセキュリティ向上策について、電力SWGにおける議論を取りまとめた提言である。これを踏まえ、電力分野で取り組むべきサプライチェーン・セキュリティ対策として、電気設備の技術基準の解釈にも引用されている「電力制御システムセキュリティガイドライン」の見直しを含め、効果的かつ実効性のある方策を検討・導入していくことが望ましい。あわせて、上記ガイドラインへの対応を進め、自己点検及び外部有識者を交えた取組の客観的なレビュー等の継続的な実施が望まれる。

1. サプライチェーン・リスク管理	• 電力制御システム等に関連する委託先等の役割と責任範囲を明確化 • 電力制御システム等のサプライチェーンの依存関係及び委託先等のセキュリティ対策状況の把握
	• リスク分析手法の選択 • 資源エネルギー庁「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」等の活用
2. セキュリティ仕様の確認	• 電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にする • 電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する • セキュリティに影響を与える可能性がある変更を適切に管理する
3. 機器・外部記憶媒体※1の管理	• 電力制御システム等に関わる機器・外部記憶媒体を、システムライフサイクル（運用・保守段階だけでなく、廃止段階も含む）を通じて管理し、保護する

※1 「電力制御システムセキュリティガイドライン」では、「機器」とは、システムを構成するサーバー、パソコンや可搬型の機器等の端末及びネットワークの構成機器をいい、「外部記憶媒体」とは、機器に接続してそのデータを保存するための可搬型の装置をいう。

出所）電力SWG, 電力制御システムのサプライチェーン・セキュリティ向上策に関する提言 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf

サプライチェーン・リスクへの対策に関する手引き文書について

- 「電力制御システムセキュリティガイドライン」の記載内容は事業者に対する要求事項であり、対策の実施に向けた具体的な取組等は含まれない。
- 中小規模の事業者をはじめ、多くの事業者がサプライチェーン・リスクに対する対策に課題を抱えているところ、**「電力制御システムセキュリティガイドライン」の要求事項への対応を促進するには、具体的な対策手順等を示す**ことが効果的ではないか。
- そのため、**サプライチェーン・リスクに対する事業者の対応を支援する具体的な対策手順等を示した手引き文書を作成**することとしたい。

サプライチェーン・リスクへの対策に関する手引き文書のイメージ

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	
1. サプライチェーン・リスク管理	• 電力制御システム等に関連する委託先等の役割と責任範囲を明確化 • 電力制御システム等のサプライチェーンの依存関係及び委託先等のセキュリティ対策状況の把握
	• リスク分析手法の選択 • 資源エネルギー庁「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」等の活用
2. セキュリティ仕様の確認	• 電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にする • 電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する • セキュリティに影響を与える可能性がある変更を適切に管理する
3. 機器・外部記憶媒体の管理	• 電力制御システム等に関わる機器・外部記憶媒体を、システムライフサイクル（運用・保守段階だけでなく、廃止段階も含む）を通じて管理し、保護する

それぞれの要求事項に対して、
対策の実施に当たっての手引き（ガイド）と、
対策のプラクティスを整理

（参考）サプライチェーン・リスクへの対策に関する手引き文書の目次のイメージ

1. 背景と目的
- 1.1. 背景
- 1.2. 目的
- 1.3. 主な対象読者
- 1.4. 本文書の活用方法

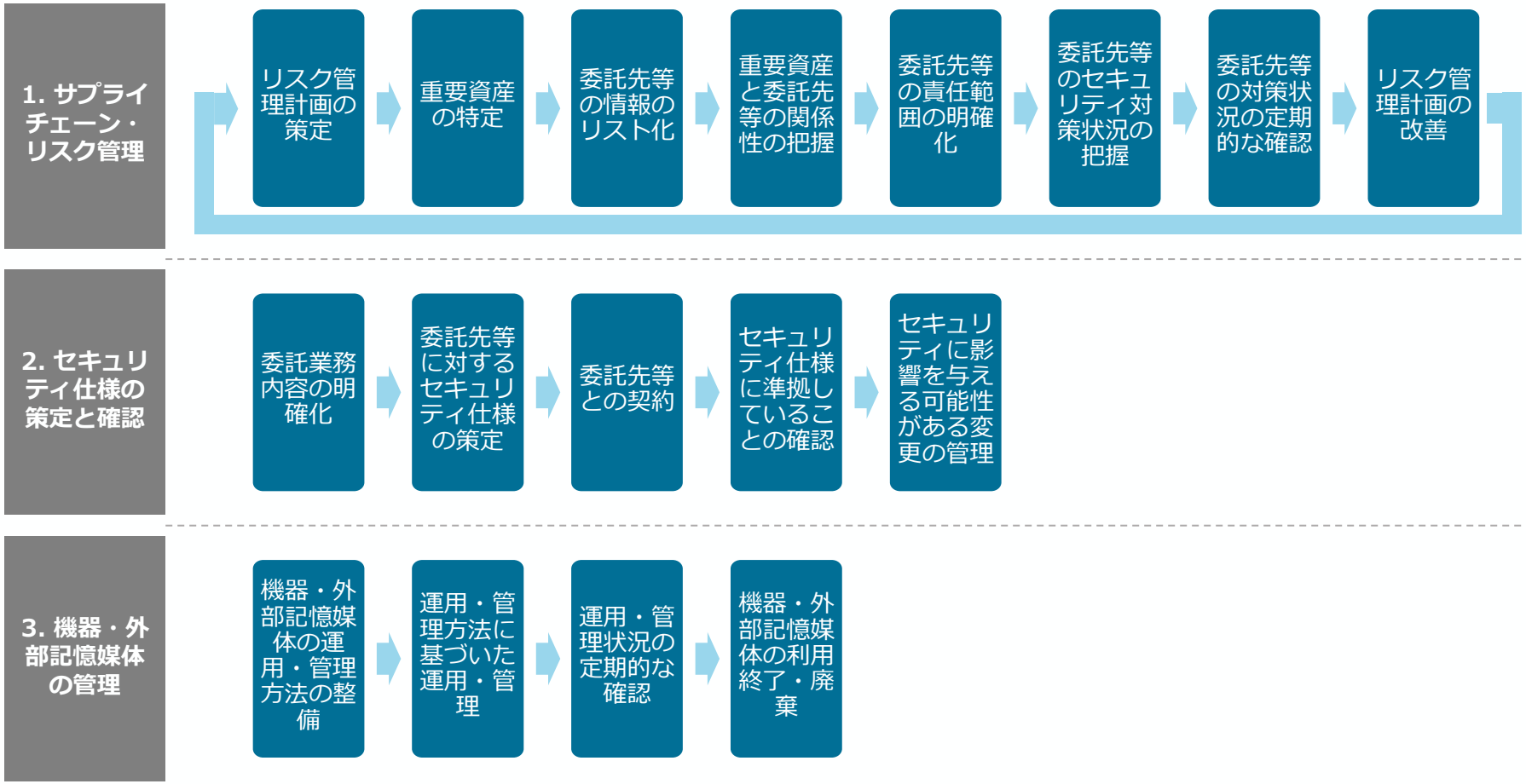
2. 求められるサプライチェーン・セキュリティ対策
- 2.1. 対応すべきサプライチェーン・リスク
- 2.2. 求められるサプライチェーン・セキュリティ対策
- 2.3. 想定される対応プロセス

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策定と確認」に関する対策の手引き・プラクティス
- 3.3. 「3. 機器・外部記憶媒体の管理」に関する対策の手引き・プラクティス

4. 付録
- 4.1 用語集
- 4.2 参考文書

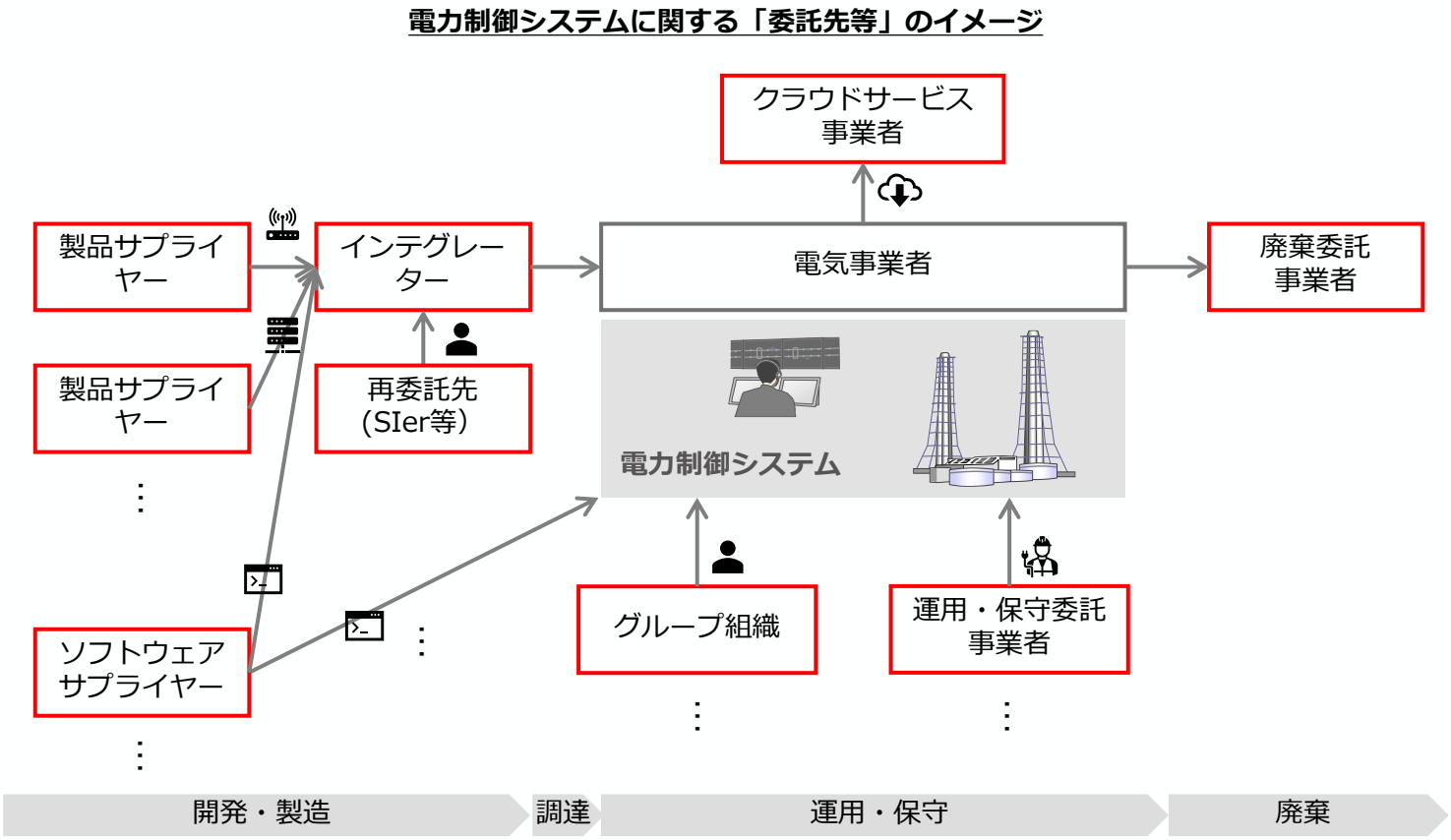
（参考）手引き文書における対応プロセスのイメージ

- 各取組に対して想定される対応フローを整理したうえで、各プロセスにおける具体的な対策の手引きや、対策に関するグッドプラクティスを示す。



（参考）手引き文書で対象とする「委託先等」のイメージ

- 「電力制御システムセキュリティガイドライン」の定義に則り、本手引きで考える「委託先等」とは「委託先、再委託先及び発注先」を指し、機器・システムの発注先だけでなく、運用・保守に関する委託事業者や廃棄委託事業者も含む。



本日、御議論いただきたいことについて

- 今後、手引き文書の策定に向け、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の対応フローを整理し、**事業者等に対するヒアリングや既存関連文書の調査結果を踏まえ、各プロセスにおける具体的な対策の手引きやグッドプラクティスを整理**していく。
- 本日の電力SWGでは、**手引き文書に記載すべき項目等をはじめとする全体構成について、御意見を伺いたい**。
- 加えて、**事業者に求められる以下の3つの内容について、具体的に求められる対応や対策の参考となるプラクティス等について、御意見を頂戴したい**。
  - 1. サプライチェーン・リスク管理
  - 2. セキュリティ仕様の策定と確認
  - 3. 機器・外部記憶媒体の管理