

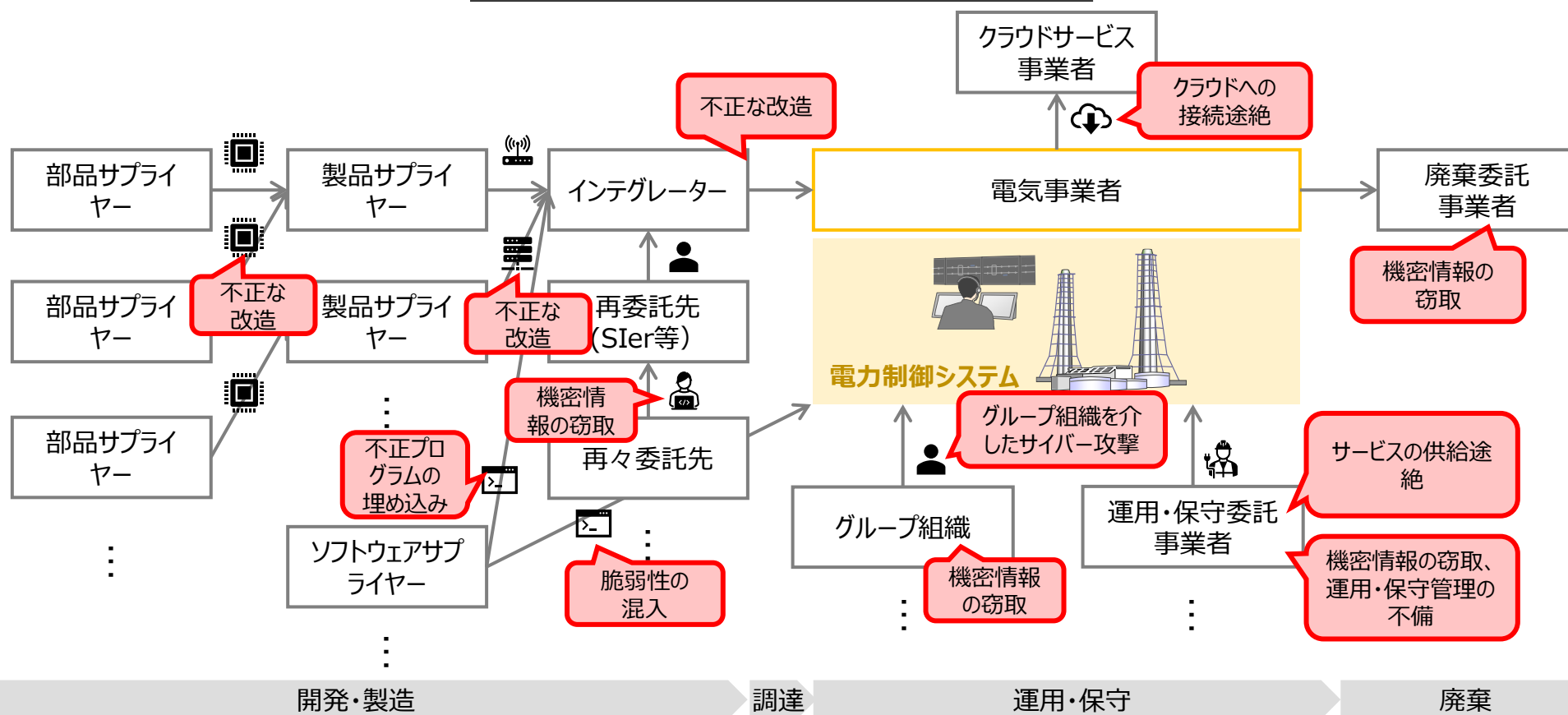
電力制御システムにおける サプライチェーン・リスクに対する対応について

2024年 2月 1日

本SWGで議論する「サプライチェーン・リスク」

- NISCの文書を参照し、本SWGでは、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係る一連の工程に加え、調達・運用・保守・廃棄を含むライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスクを「サプライチェーン・リスク」と呼ぶ。
(自然災害に起因するサプライチェーンの途絶等は、本日のSWGのスコップ外とする。)

電力制御システムに想定されるサプライチェーン・リスクの例



※ 「リスク」とは、脅威と脆弱性の合致により損失が発生する可能性、また、その損失をいう。

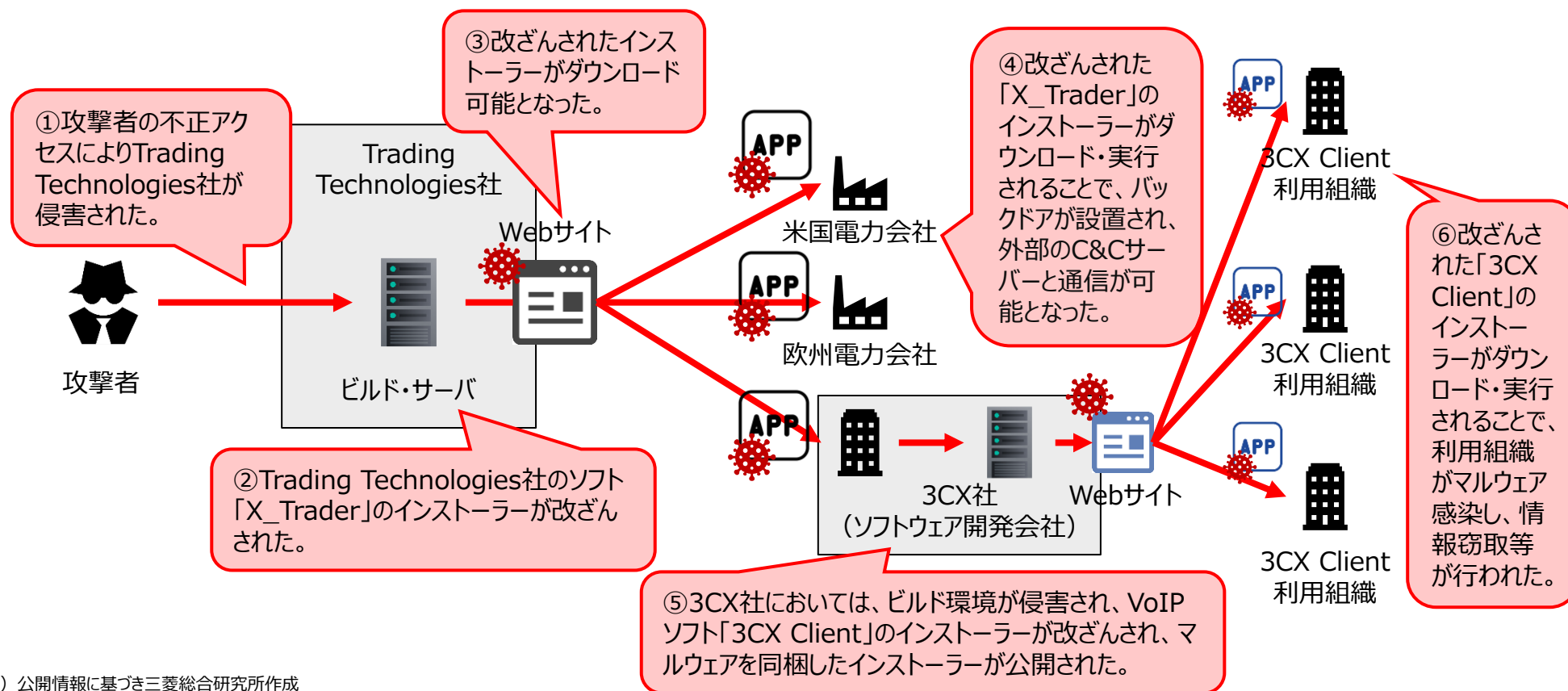
出所) NISC、外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書等に基づき作成 <https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf>

【サプライチェーンを通じたサイバー攻撃の事例（電力分野）】

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、同社が販売する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した。

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

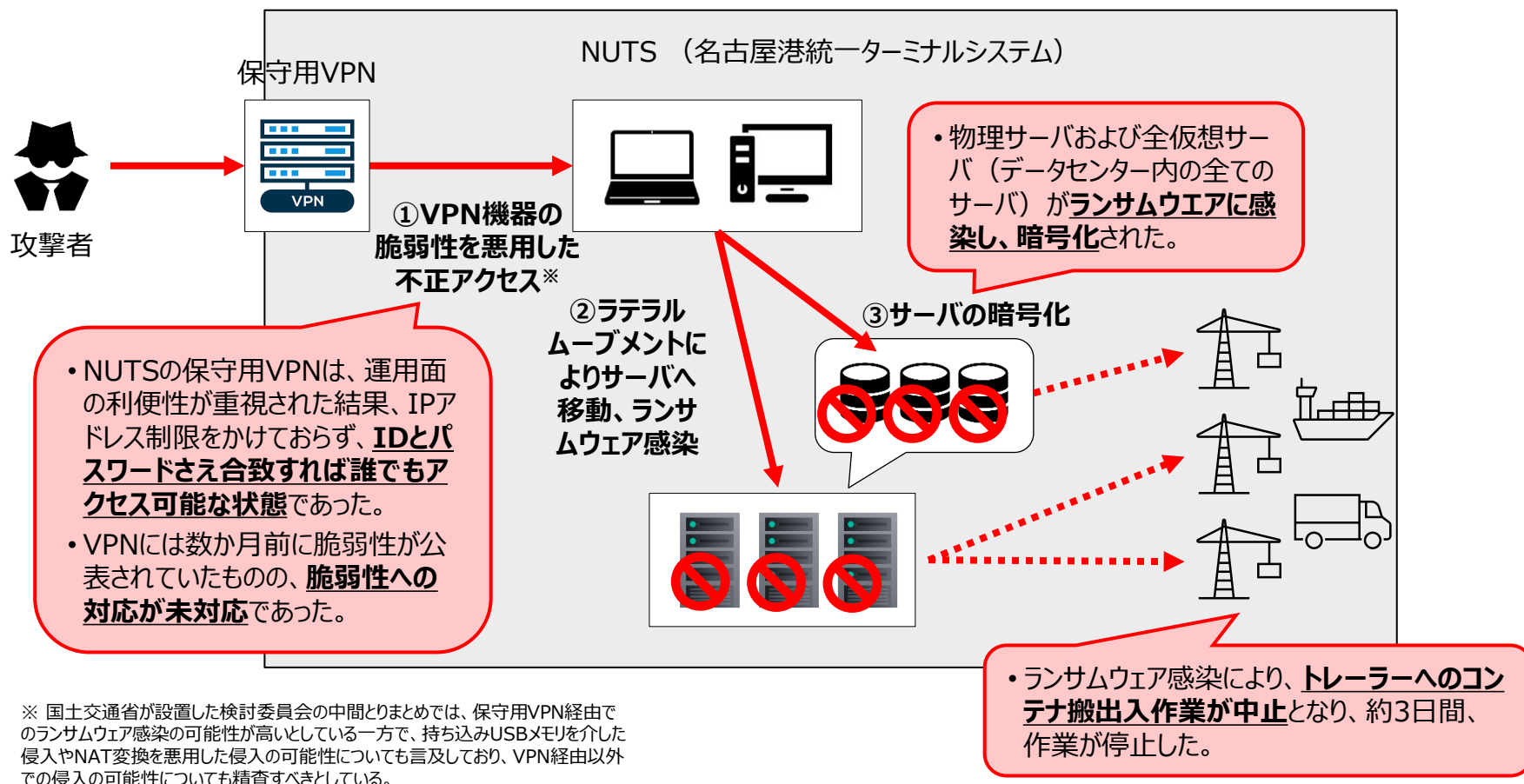


【サプライチェーンを通じたサイバー攻撃の具体的事例（港湾分野）】

名古屋港コンテナターミナルに対するランサムウェア攻撃

- 2023年7月4日、名古屋港コンテナターミナルのシステムがランサムウェア攻撃を受け、物理サーバ及びデータセンター内の全仮想サーバが暗号化されたことで、およそ3日間にわたりターミナルの操業が停止した。
- 攻撃経路について、VPN機器の脆弱性を悪用され、不正アクセスされた可能性が高いとしている。

名古屋港コンテナターミナルに対するランサムウェア攻撃のイメージ

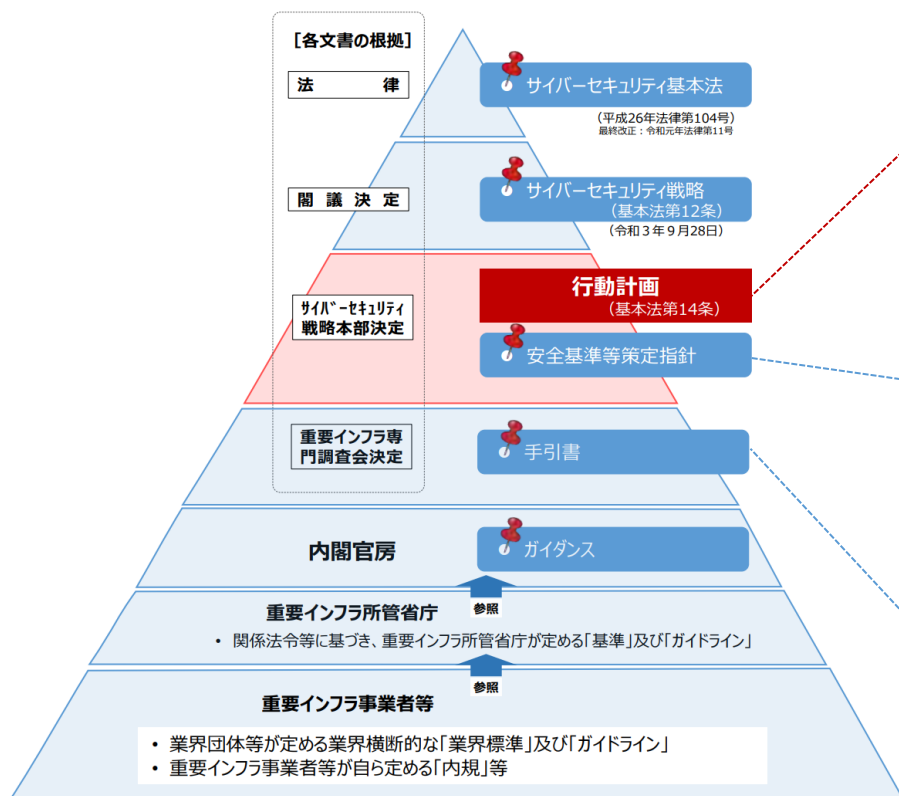


国内電力分野に関連する取組状況

(1) NISC：重要インフラ防護に関する安全基準等の改訂

- NISCは、令和4年に策定した「重要インフラのサイバーセキュリティに係る行動計画」において、サプライチェーン・リスク対応に関して、安全基準等策定指針の記載を充実させる方針を示した。
- この方針を踏まえ、令和5年に策定した「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」では、**サプライチェーン・リスクに関するリスクアセスメント・対応等が、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確保に向けた取組として明記**された。

重要インフラ防護に関する安全基準等に係る体系、各文書におけるサプライチェーン・リスク関連の記載状況



重要インフラのサイバーセキュリティに係る行動計画（令和4年6月）

- ・ 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進するための行動計画
- ・ サプライチェーン・リスクへの対応について安全基準等策定指針の記載を充実させる方針を示す

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（令和5年7月）

- ・ 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況把握、**サプライチェーン・リスクに関するリスクアセスメント及びリスク対応等について、重要インフラ分野共通して求められるサイバーセキュリティ確保に向けた取組として新たに記載**

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（令和5年7月）

- ・ サプライチェーン・リスク対応として、製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理すること、不正機能等の埋め込みに係る脅威に対応すること等の取組を整理・記載

国内電力分野に関連する取組状況

(1) NISC：重要インフラ防護に関する安全基準等の改訂

- 「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、対応すべき代表的なサプライチェーンに係る脅威として、
 - ・不正機能等の埋め込み
 - ・サービスの供給途絶
 - ・外部サービスにおける情報の不適切な取扱い
 - ・海外拠点、グループ組織、取引先等を経由したサイバー攻撃の4つの脅威を示した上で、以下の取組を、各重要インフラ分野に共通して求められるサプライチェーン・リスクマネジメントの取組として位置づけている。

安全基準等策定指針におけるサプライチェーン・リスクマネジメントに関する取組

【各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】

- 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行う。
- サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。海外拠点については、現地の法令、文化等も踏まえた対応を行う。
- 直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。

【組織状況に応じて採否が検討されうる取組（推奨事項）】

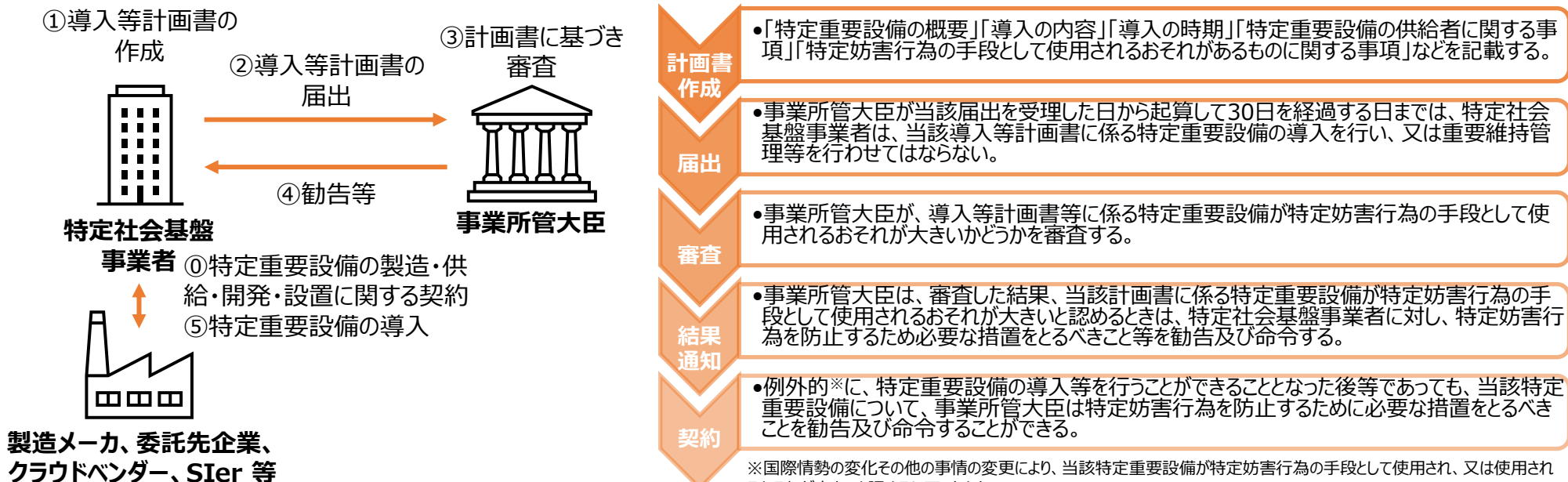
- リスクに応じて直接の供給者に連なる供給者への関与の程度を決定しつつ、各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。
- セキュリティ対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めることが望ましい。

国内電力分野に関連する取組状況

(2) 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する制度

- 2022年5月に成立した経済安全保障推進法では、**特定社会基盤事業者が特定重要設備の導入及び重要維持管理等の委託を行う場合、事業所管大臣の審査を受けなければならない**としており、2024年5月17日より運用が開始される。
- 審査において、特定重要設備が特定妨害行為（我が国の外部から行われるサイバー攻撃、物理的な妨害行為等）の手段として使用されるおそれが大いだと認められたとき、**事業所管大臣は、特定妨害行為を防止するため必要な措置をとるべきこと等を勧告及び命令**することができる。
- 2023年11月16日、**電力分野では特定の基準を満たす42者が特定社会基盤事業者として指定**され、特定重要設備の導入及び重要維持管理等の委託を行う場合、**経済産業大臣による事前審査が必要**となる。

「特定重要設備」の導入に係る事前審査のプロセス



国内電力分野に関連する取組状況

(2) 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する制度

- 特定社会基盤事業者が作成する導入等計画書には、「**特定重要設備の概要**」「**導入の時期/委託の時期又は期間**」「**特定重要設備の供給者に関する事項/重要維持管理等の委託の相手方に関する事項**」「**特定重要設備の導入/重要維持管理等の委託に当たって特定社会基盤事業者が講ずる特定妨害行為を防止するための措置に係る事項（リスク管理措置）**」を記載する必要がある。
- 加えて、特定重要設備の導入時には「特定重要設備の一部を構成する設備、機器、装置又はプログラムであって特定妨害行為の手段として使用されるおそれがあるもの（構成設備）に関する事項」、重要維持管理等の委託時には「重要維持管理等の委託の相手方が他の事業者に再委託して重要維持管理等を行わせる場合にあっては、当該再委託に関する事項」（※）を記載する必要がある。

（※）重要維持管理等の委託の相手方が他の事業者に再委託して重要維持管理等を行わせる場合

導入等計画書における記載事項

事項	特定重要設備の導入を行う場合	特定重要設備の重要維持管理等を行わせる場合
特定重要設備の概要	種類、名称、機能、設置場所、使用場所	種類、名称、機能、設置場所、使用場所
導入の内容及び時期/ 委託の内容及び時期又は期間	導入の目的、導入に携わる者の名称等、導入の時期	委託の目的、委託の内容・場所、委託の時期又は期間
特定重要設備の供給者に関する事項/重要維持管理等の委託の相手方に関する事項	供給者の名称・住所・設立準拠法等、供給者の議決権の5%以上を保有する者、供給者の役員の氏名・生年月日・国籍等、（供給者が、外国政府等との取引が売上高の25%以上を占める場合）外国政府等の名称等、設備の製造場所の所在地	相手方の名称・住所・設立準拠法国等、相手方の議決権の5%以上を保有する者、相手方の役員の氏名・生年月日・国籍等、（相手方が、外国政府等との取引が売上高の25%以上を占める場合）外国政府等の名称等
構成設備に関する事項/重要維持管理等の再委託に関する事項	構成設備の概要（種類・名称・機能）、供給者の名称・住所・設立準拠法国、供給者の議決権の5%以上を保有する者、供給者の役員の氏名・生年月日・国籍等、（供給者の外国政府等との取引が当該供給者の売上高全体の25%以上を占める場合）取引先の外国政府等の名称等、構成設備の製造場所の所在地	再委託の内容・場所・時期又は期間、相手方の名称・住所・設立準拠法国、相手方の議決権の5%以上を保有する者、相手方の役員の氏名・生年月日・国籍等、（相手方の外国政府等との取引が当該相手方の売上高全体の25%以上を占める場合）取引先の外国政府等の名称等
リスク管理措置	導入に関するリスク管理措置	重要維持管理等の委託に関するリスク管理措置

出所）特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律 <https://elaws.e-gov.go.jp/document?lawid=504AC0000000043>

経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyou.pdf

海外電力分野におけるサプライチェーン・リスクに関する規制状況

- 海外では、罰則規定のある法規制において、電力会社におけるサプライチェーン・リスク管理を求めている。
- ドイツでは、一部の電力会社に対して、導入する重要部品に関する政府への事前通知・審査を求めている。
- また、英国では、一部の電力会社に対して、サプライヤー契約に関する政府への通知を求めている。

海外電力分野におけるサプライチェーン・リスクに関する規制状況

国・地域				
法規制	連邦電力法	- ITセキュリティ法2.0 - エネルギー産業法 - BSI法	- NIS規則 - 国家安全保障・投資法（NS&I Act）	- NIS指令/NIS2指令 - EU Regulation No. 2019/943
要件文書	NERC CIP-013: Cyber Security - Supply Chain Risk Management	ITセキュリティカタログ（IT-Sicherheitskatalog）	- NIS Guidance - Cyber Assessment Framework (CAF)	- EU各国の国内法により規程 - Network Code on Cybersecurity
所管組織	- FERC（連邦エネルギー規制委員会） - NERC（北米電力信頼度協議会）	- BSI（連邦情報セキュリティ庁） - BMI（連邦内務省） - BNetzA（連邦ネットワーク庁）	- NCSC（国家サイバーセキュリティセンター） - Ofgem（ガス・電力市場局） - BEIS（ビジネス・エネルギー・産業戦略省）	- EU各国の所管省庁 - ENTSO-E
電力会社に求められるサプライチェーン・リスク対策	<u>サプライチェーン・リスク管理の実施</u> - サプライチェーン・リスク管理計画の定期的な見直し（少なくとも15ヶ月に一度） - サプライチェーン・リスク管理状況のNERCへの報告	<u>サプライチェーン・リスク管理の実施</u> <u>導入する重要部品に関する政府への事前通知・審査</u> - インシデント情報等に関する政府への報告	<u>サプライチェーン・リスク管理の実施</u> - 対策状況に関する政府への定期的な報告 - サプライヤー契約に関する政府への通知 - 政府による調査・介入への協力	<u>サプライチェーン・リスク管理の実施</u> - 人的サプライチェーンへの対策（産業スパイへの対策、企業秘密の保護など） <u>委託先や導入部品のサイバーセキュリティ対策の検証</u>
罰則等	違反度合いに応じた罰則規程あり	最大2,000万ユーロ（約30億円）又は企業の全世界売上高の4%のいずれか高い方の罰金	最大1,700万ポンド（約30億円）の罰金	NIS2指令では、最大1,000万ユーロ（約15億円）又は企業の全世界売上高の2%のいずれか高い方の罰金

電力制御システムにおけるサプライチェーン・リスクに対する対応について

- 重要インフラ分野全体において、サプライチェーンにおける信頼（トラスト）の確保が求められるところ、国内電力分野におけるサプライチェーン・リスクに対する対応高度化に向けた取組は必要不可欠である。
- 一方で、現状の「電力制御システムセキュリティガイドライン」では、委託先等の対応を求めているものの、明示的に「サプライチェーン・リスク」に関する言及は無く、サプライチェーン・リスクに対する対策を求めているわけではない。
- NISCの「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」の改訂を踏まえ、来年度、日本電気協会及び電事連を中心に「電力制御システムセキュリティガイドライン」の改訂作業が行われる予定であるところ、この改訂に合わせて、電力制御システムにおけるサプライチェーン・リスクへの対応を「電力制御システムセキュリティガイドライン」において求めるべきではないか。
- また、実効性のある対策を電力業界に求めていくために、資料5-2に示す提言を電力SWG名義で発表してはどうか。

電力制御システムにおいて求められるサプライチェーン・リスク対策（案）

- 電力制御システムに想定されるサプライチェーン・リスクに対応するために、NISC安全基準等策定指針、経済安全保障推進法及び現行の電力制御システムセキュリティガイドラインの内容を踏まえ、**以下のような対策を事業者に求めていくべきではないか。**

項目	事業者に求めていくべきサプライチェーン・リスク対策（案）	対応するサプライチェーン・リスク
サプライチェーン・リスク管理	● 委託先等の対応に関して、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にする。 ● 電力制御システム等における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を把握する。 ● 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。	全リスク
セキュリティ仕様の確認	● 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 ● 仕様への準拠性の確認に関して、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。 ● 電力制御システム等の仕様変更に関して、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。	・ 開発・製造時の不正な改造 ・ 開発・製造時の不正プログラムの埋め込み ・ 運用・保守時のソフトウェアの不正な更新
機器・外部記憶媒体の管理	● 機器・外部記憶媒体の管理に関して、機器・外部記憶媒体をライフサイクルを通じて管理し、保護する。	・ 調達時の不正な改造 ・ 調達時の不正プログラムの埋め込み ・ 廃棄時の機密情報の窃取

【用語の定義（電力制御システムセキュリティガイドラインより引用）】

- ・ 委託先等：委託先、再委託先及び発注先をいう。
- ・ 機器：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う。
- ・ 電力制御システム：電力の安定供給、電気工作物の保安（公衆安全を含む）の確保に資するために、電気事業の用に供する電気工作物を監視・制御する機能等を具備したシステムをいう。
- ・ 電力制御システム等：電力制御システム及び電力制御用ネットワークの全体をいう。
- ・ 電力制御用ネットワーク：電力制御システム同士をつなぐネットワーク又は制御箇所と被制御箇所を結ぶネットワークをいう。
- ・ セキュリティ仕様：電力制御システム等の機能要件に応じて策定されたセキュリティ要件をいう。
- ・ ライフサイクル：電力制御システム等の計画・開発・調達・運用・保守・廃止をいう。

(参考) 現行の電制ガイドラインの記載内容との対比

項目（案）	事業者に求めていくべきサプライチェーン・リスク対策（案） ※ 赤字が現行ガイドラインからの主要な差分	現行の電力制御システムセキュリティガイドラインの記載事項
サプライチェーン・リスク管理	委託先等の対応に関して、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にする。	【第2-2条 役割】 電力制御システム等に関連する委託先等の役割を明確にすること。
	電力制御システム等における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を把握すること。	—
	電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。	—
セキュリティ仕様の確認	電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。	【第6-1条 セキュリティ仕様の確認】 1. セキュリティ仕様 電力制御システム等の調達時にセキュリティ仕様を明確にすることが望ましい。
	仕様への準拠性の確認に関して、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。	【第6-1条 セキュリティ仕様の確認】 2. 準拠性の確認 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ことが望ましい。
	電力制御システム等の仕様変更に関して、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。	【第6-1条 セキュリティ仕様の確認】 3. 仕様変更 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ことが望ましい。
機器・外部記憶媒体の管理	機器・外部記憶媒体の管理に関して、機器・外部記憶媒体をライフサイクルを通じて管理し、保護する。	【第6-2条 機器・外部記憶媒体及びデータの管理】 1. 機器・外部記憶媒体の管理 機器・外部記憶媒体を管理し、保護することが望ましい。

(参考) 国内外の取組との対応

項目 (案)	事業者に求めていくべきサプライチェーン・リスク対策 (案)	 NISC安全基準等策定指針	 経済安全保障推進法※	 NERC CIP基準	 NIS2指令
サプライチェーン・リスク管理	- 委託先等の対応に関して、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にする。 - 電力制御システム等における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を把握する。 - 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。	- 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行う。 - サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。海外拠点については、現地の法令、文化等も踏まえた対応を行う。 - 直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。 - リスクに応じて直接の供給者に連なる供給者への関与の程度を決定しつつ、各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。	- 特定重要設備を導入する場合のリスク管理措置の項目：全般 - 特定重要設備の重要維持管理等を委託する場合のリスク管理措置の項目：全般	- NERC CIP-013-01：R1、R2、R3 - NERC CIP-013-02：R1、R2、R3 - NERC CIP-013-03 (Draft)：R1、R2、R3	NIS 2 Directive：(85)、(86)、(88)、(91)
セキュリティ仕様の確認	- 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 - 仕様への準拠性の確認に関して、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。 - 電力制御システム等の仕様変更に関して、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。	—	- 特定重要設備を導入する場合のリスク管理措置の項目：①-1、①-2、③-1、③-2、④-1、④-2、⑤-1、⑤-2、⑦、⑬ - 特定重要設備の重要維持管理等を委託する場合のリスク管理措置の項目：①、③、④、⑤、⑥、⑦	- NERC CIP-013-01：R1 - NERC CIP-013-02：R1 - NERC CIP-013-03 (Draft)：R1	NIS 2 Directive：(85)、(86)、(88)、(91)
機器・外部記憶媒体の管理	機器・外部記憶媒体の管理に関して、機器・外部記憶媒体をライフサイクルを通じて管理し、保護する。	—	—	CIP-011-01：R2	NIS 2 Directive：(91)

※ 内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」のP.13～17において記載された特定重要設備を導入する場合／特定重要設備の重要維持管理等を委託する場合のリスク管理措置の項目に基づき整理。なお、各省庁の主務省令において、個別に別途リスク管理措置を設けている場合があることに留意。https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyoubu.pdf

サプライチェーン・リスク対応の高度化に向けて

- 委員に対する事前の意見交換では、「電力制御システムセキュリティガイドライン」の改訂に限らず、日々高度化・複雑化するサプライチェーン・リスクに対応するため、より中長期的な取組についても御意見が挙げられた。
- 事前の意見交換で挙げられたサプライチェーン・リスクの状況や事業者が抱える課題を踏まえ、サプライチェーン・リスク対応の高度化に向け、既存の取組等を活用し、事業者におけるサプライチェーン・リスク対応を支援する内容（例：委託先等を含むサプライチェーン・リスクの把握方法、リスクの管理方法等）を含んだ、より詳細な手引き文書等の策定が必要ではないか。
- また、NISCの安全基準等策定指針において、サプライチェーン全体での対策実効性を高めることが言及されているところ、事業者に関しないサプライチェーン全体での教育・訓練の実施等の方策についても、検討を進めるべきではないか。