



事例調査業務

概要説明資料

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
事業推進部



1. 本調査の概要

背景・目的及び調査概要

サイバー攻撃の高度化・激化が進む中、サイバー攻撃がフィジカル領域に大きな影響を及ぼすようになり、経済活動の基盤を守るためには、プラント等の事故が発生した場合に、サイバーインシデントの観点からの原因究明可能な機能を有することが求められるようになった。

このため、2025年を目処に「サイバーインシデントに係る事故調査」機能を整備するため、国内及び欧米における「事故調査」に関する実施体制、法制度及び最新動向の調査を実施した。

上述した目的を達成するために、有識者へのヒアリング・文献・Web調査等の手段により、以下の動向調査を実施した。

- ① 欧米各国における「事故調査」及び「サイバーインシデントに係る事故調査」の動向調査
- ② 国内における重要インフラ・産業基盤の各業界における「事故調査」のしくみの調査

また、上述した動向調査の結果を踏まえて、国内において「サイバーインシデントに係る事故調査」機能を整備する上で、検討すべき事項や課題等について検討した。

2. 欧米各国における「事故調査」及び 「サイバーインシデントに係る事故調査」 の動向調査

- 2.1 電力分野
- 2.2 鉄道分野
- 2.3 航空分野
- 2.4 自動車分野

2.1 電力分野

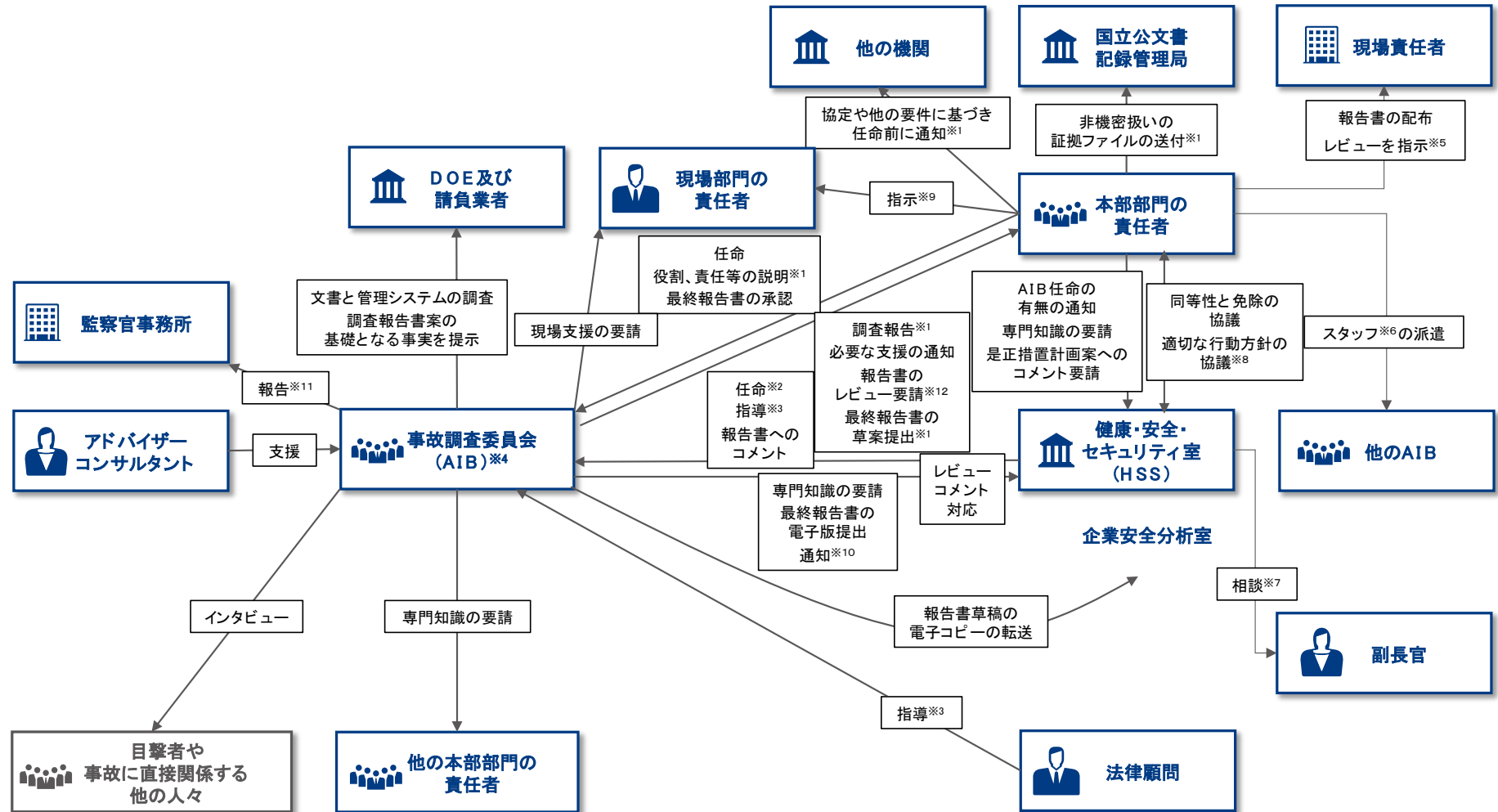
電力分野では、事故調査におけるサイバーに言及した法制度が整備されつつある。主な事故調査のスキーム図を次ページ以降に示す。

国	組織名	関連する法制度	事件事例	サイバーに関する言及	備考(ガイドライン等)
米国	エネルギー省(DOE)	DOE令 225.1B 事故調査	バンドンローグNo.1115kVラインでのウィルソン建設会社の従業員の死亡事故(2013)	○	EROイベント分析プロセス DOEハンドブック 事故及びオペレーション上の安全性分析
	北米電力信頼度協議会(NERC)	NERC 手続き規則	ワシントンD.C.エリアの低電圧障害イベント(2015)		
EU	—	NIS指令 NIS2指令	—	△※	—
英国	国家サイバーセキュリティセンター(NCSC)	NIS規則	英国電力システム障害(2019)	△※	NCSC サイバーアセスメントフレームワーク
フランス	国家情報システムセキュリティ庁(ANSSI)	必須サービス事業者及びデジタルサービス事業者のネットワーク及び情報システムのセキュリティに関する政令	—	△※	—
ドイツ	連邦情報セキュリティ局(BSI)	NIS指令の実施に関する法律 ITセキュリティ法2.0 BSI法	—	△※	—
エストニア	エストニア情報システム局	サイバーセキュリティ法	—	△※	—

【凡例】○:あり / △:一部あり / -:なし(公開情報ベース)

※本表で取り上げているNIS指令やそれに関する各国の法律は、電力事業者に限らず基幹サービス運営者を対象としている。

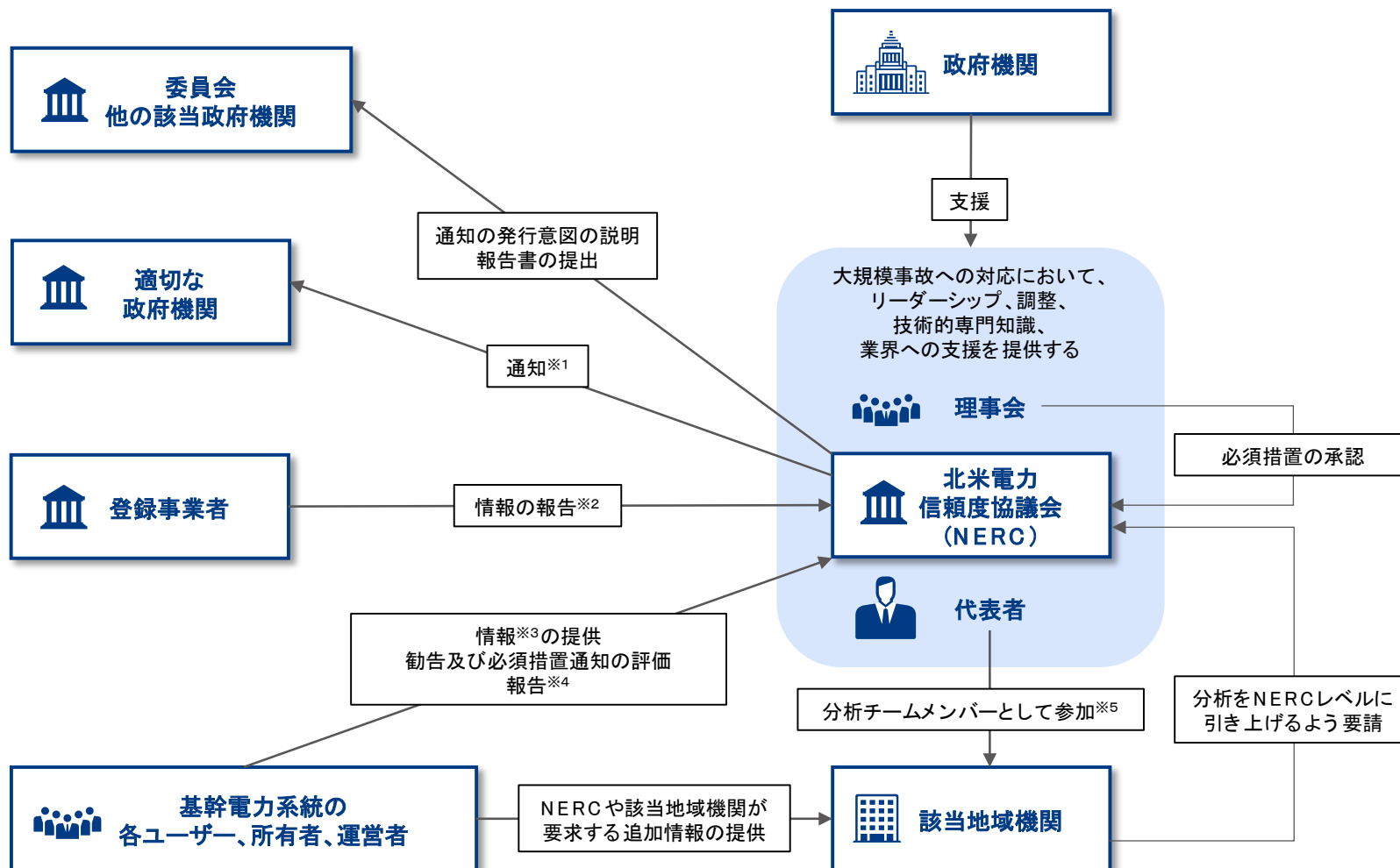
2.1 電力分野 米国DoE 事故調査スキーム図



※1: HSSがAIBを任命した場合はHSSが担う。
 ※2: 本部部門の責任者とHSSがDOEの利益になると合意した場合。
 ※3: 事故調査中にC.F.R.と本命令の間に矛盾が確認された場合。
 ※4: 議長及び3〜6名のメンバーで構成される。全メンバーがDOE連邦職員であり、少なくとも一人はDOE事故調査官。
 ※5: 事故調査で特定された問題点のうち、作業場所や業務に適用可能なものについては、条件の範囲のレビューを行う。
 ※6: AIB議長やDOE事故調査官を務める訓練を受けた有資格者。
 ※7: AIBを任命しないという本部部門の責任者の決定に同意しない場合

※8: 報告書で原因となる要因が特定されなかった場合、再発防止のための適切な是正措置を特定するための適切な行動方針について協議する。
 ※9: 本部部門の責任者の指示に従い、現場部門の責任者の権限下にある作業場所や活動に適用される可能性のある事故調査から得られた特定の問題について、条件の範囲のレビューを実施し、他のDOEサイトで実施された調査から得られた適用可能な教訓に対処する。
 ※10: 調査中に特定された潜在的な規制違反の問題の通知
 ※11: 事故調査の過程で確認された犯罪行為もしくは違法行為の疑いについての申し立てや証拠の報告
 ※12: AIB議長が要請する。

2.1 電力分野 米国NERC 事故調査スキーム図



※1: 物理セキュリティやサイバーセキュリティが重大事故の原因や一因として疑われる重大事故に対応する場合。NERCは直ちに適切な政府機関に通知し、その活動を調整する。

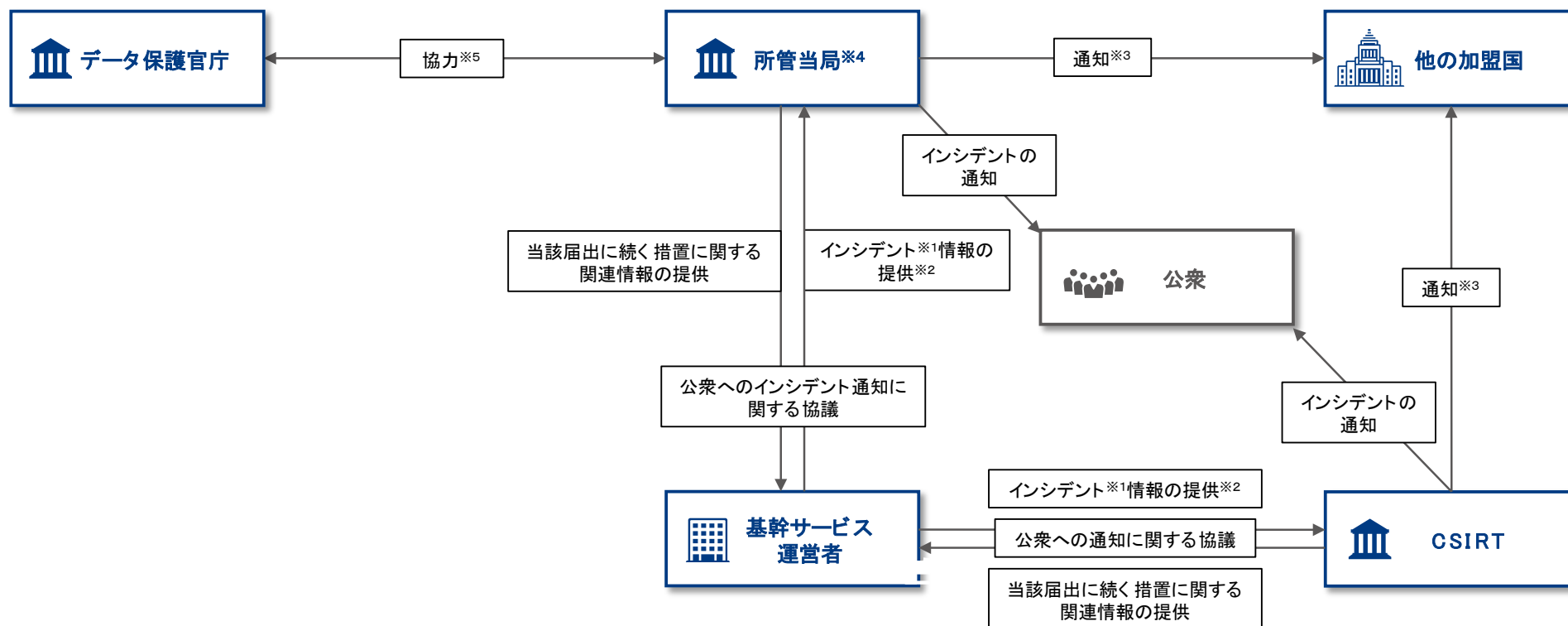
※2: 信頼性基準が、その信頼性基準に記載されている基幹電力システムの障害及び事故を報告するための特定の基準や手順を定めている限りにおいて、その信頼性規格の要件の対象となるすべての登録事業者は、指定された期間内に、その信頼性基準が要求する情報を報告しなければならない。

※3: NERCや該当地域機関が要求する追加情報や運用経験情報及びデータ。

※4: 取られた行動と、勧告及び必須措置で提起された問題の解決に向けた進捗状況のタイムリーな情報について報告。

※5: 大規模事故が単一の地域機関に限定されている場合。

2.1 電力分野 EU NIS指令によるインシデント報告スキーム図



※1: 提供する基幹サービスの継続性に重大な影響を及ぼすインシデント
 ※2: 当該インシデントによる国境を越える影響の確定を可能とする情報を含まなければならない
 ※3: インシデントが他の加盟国における基幹サービスの継続性に重大な影響を及ぼす場合

※4: ネットワーク・情報システムの安全に関する
 ※5: 個人データを侵害するインシデントへの対処に関して

2.2 鉄道分野

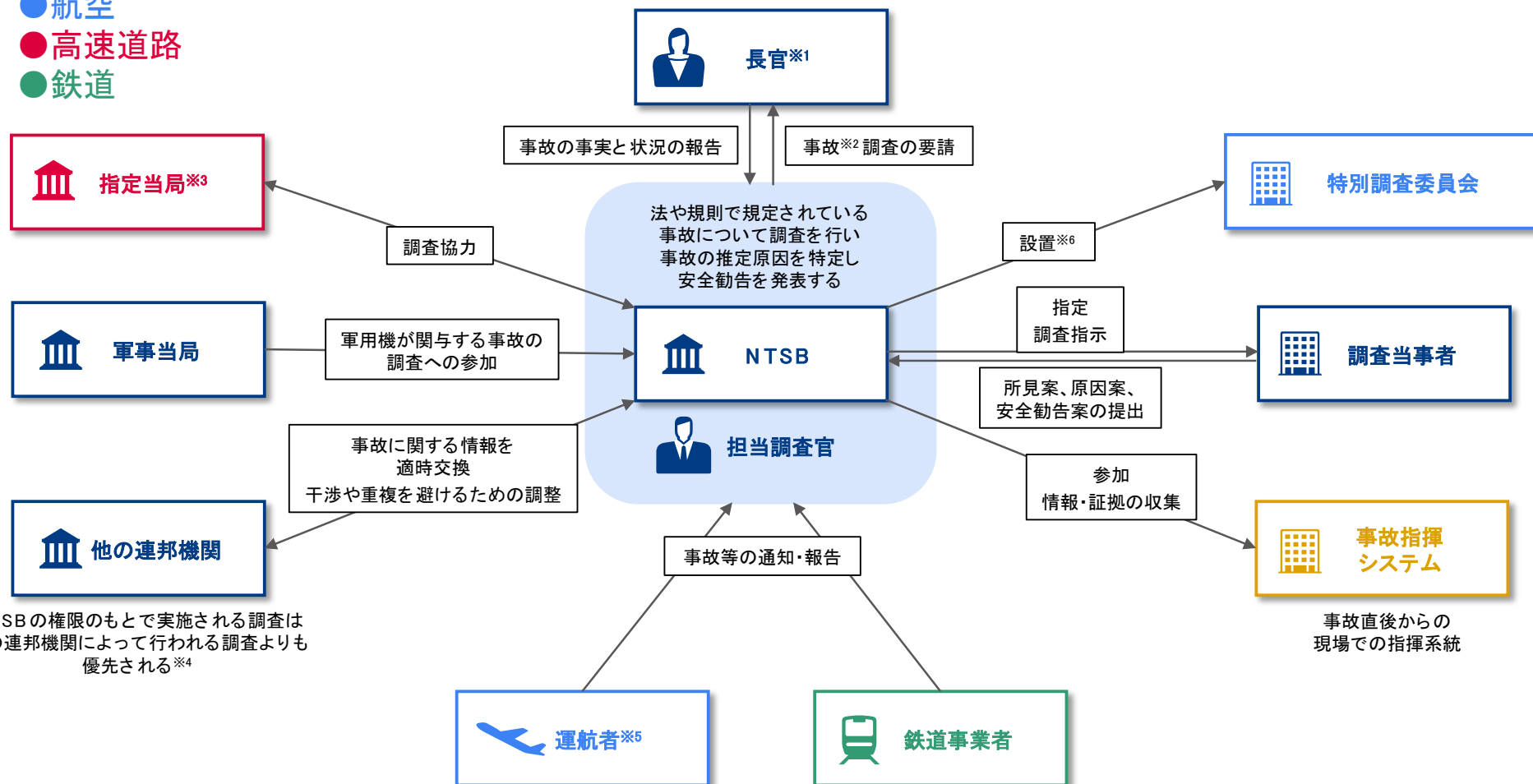
鉄道分野では、米国において事故調査におけるサイバーを含めた法制度の整備が進んでいる。主な事故調査のスキーム図を次ページ以降に示す。

国	組織名	関連する法制度	事故事例	サイバーに関する言及	備考(ガイドライン等)
米国	国家運輸安全委員会 (NTSB)	独立安全委員会法、連邦規則、セキュリティ指令1580-21-01、セキュリティ指令1582-21-01、	CSX輸送の貨物列車2両の衝突事故 (2019)	○	調査当事者向けの情報及びガイダンス 陸上輸送 IC-2021-01
EU	※各国に調査機関の設立を要請	欧州議会及び欧州理事会の指令 (EU) 2016/798	—	—	—
英国	鉄道事故調査局 (RAIB)	欧州議会及び欧州理事会の指令 (EU) 2016/798 鉄道運輸安全法 2003、 鉄道 (事故調査・報告) 規則 2005	ロンドンのワンステッドパーク近くの貨物列車の脱線 (2020)	—	—
フランス	陸上交通事故調査局 (BEA-TT)	運輸法	サンティエヌヌの302号踏切で発生した地域急行列車と軽自動車の衝突事故 (2019)	—	—
ドイツ	連邦鉄道事故調査委員会 (BEU)	欧州議会及び欧州理事会の指令 (EU) 2016/798 鉄道事故調査の再編に関する法律、 鉄道事業における危険有害事象の調査に関する規則	ミュルハイム (バーデン州)-シュリーゲン間の列車衝突事故 (2020)	—	—
エストニア	安全調査センター (OJK)	欧州議会及び欧州理事会の指令 (EU) 2016/798、 鉄道法、安全調査手順、安全調査センター規程、 事故、重大な事故、インシデントの通知手順と通知書及び報告書の形式	クルナ踏切事故 (2018)	—	—

【凡例】○:あり / —:なし(公開情報ベース)

2.2 鉄道分野 米国NTSB 事故調査スキーム図

- 航空
- 高速道路
- 鉄道



NTSBの権限のもとで実施される調査は他の連邦機関によって行われる調査よりも優先される*4

※1：運輸長官または沿岸警備隊が活動している部門の長官

※2：NTSBの調査対象であり、政府による不法行為や義務不履行が申し立てられていない事故

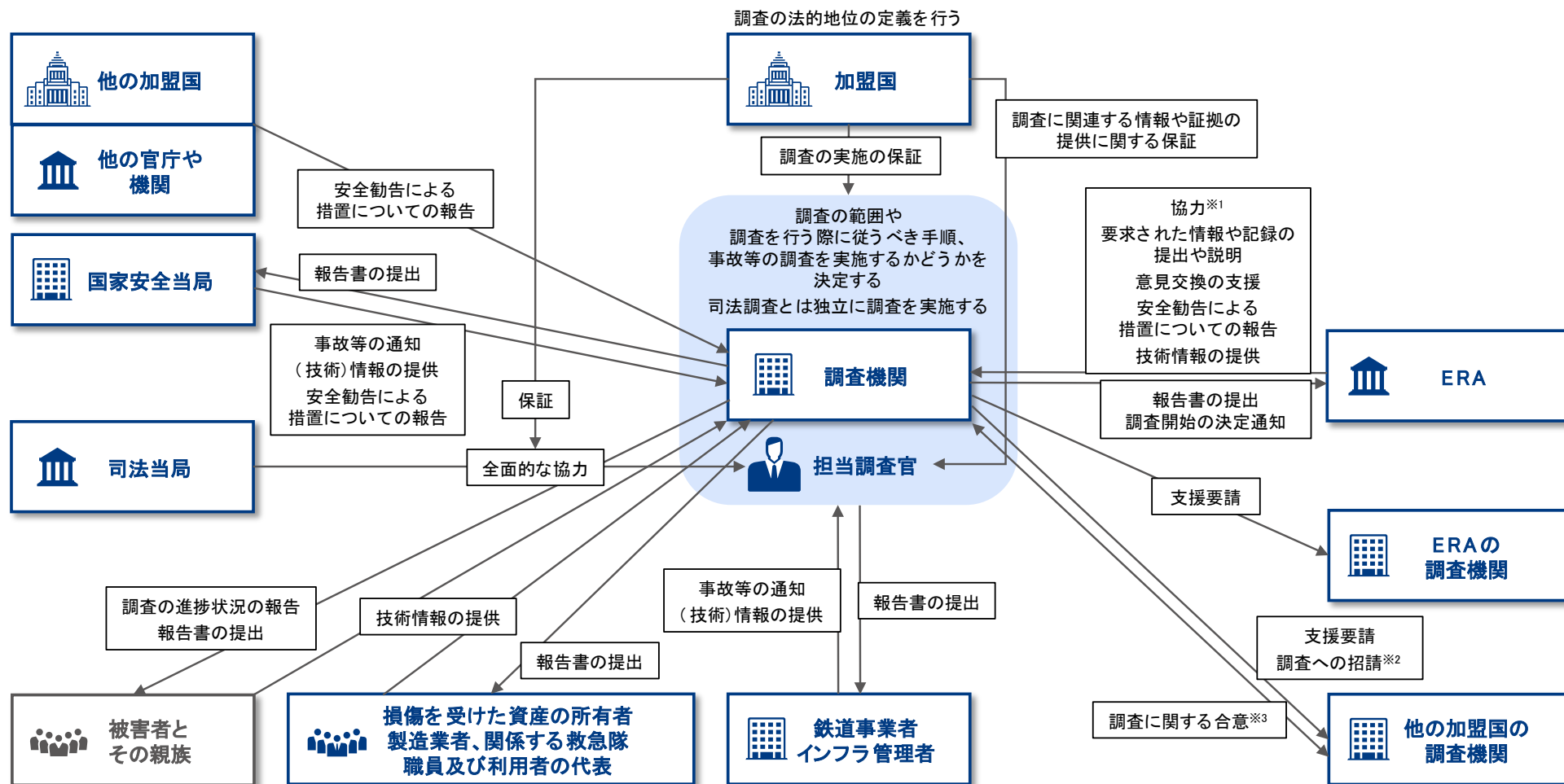
※3：事故が発生した州や地方自治体の指定当局

※4：意図的な犯罪行為によって引き起こされた可能性がある場合は除く

※5：民間航空機の運航者、米国の軍隊や諜報機関による運用でない公共航空機の運航者、外国の航空機の運航者

※6：事故が航空輸送の公安に関する重大な問題を含んでいる場合

2.2 鉄道分野 EUにおける鉄道事故調査のスキーム図



※1: 調査にERAが認可した車両やERAが認定した鉄道事業者が関与する場合

※2: 他の加盟国で設立され認可された鉄道事業者が、事故や事件に関与している場合、もしくは他の加盟国のいずれかで登録や維持されている車両が、事故や事件に関与している場合。

※3: どの加盟国で発生したかを特定することができない場合や2つの加盟国間の国境施設上もしくはその近くで発生した場合、関連する調査機関は、どちらが調査を実施するか、もしくは相互に協力して調査を実施するかについて合意しなければならない。

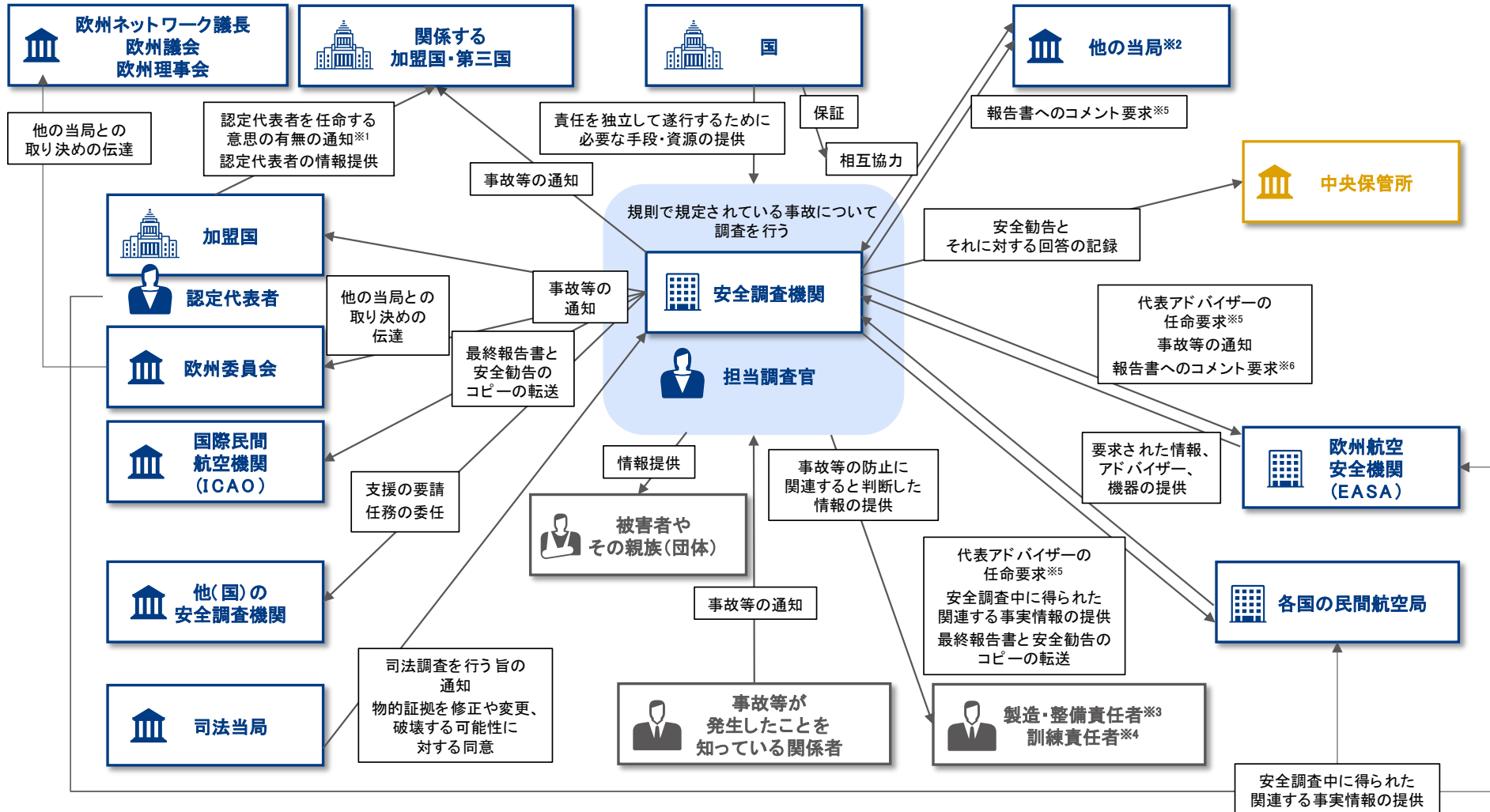
2.3 航空分野

航空分野では、米国において事故調査におけるサイバーを含めた法制度の整備が進んでいる。主な事故調査のスキーム図を次ページ以降に示す。

国	組織名	関連する法制度	事件事例	サイバーに関する言及	備考(ガイドライン等)
米国	国家運輸安全委員会 (NTSB)	独立安全委員会法、連邦規則、附属書13 航空機の事故とインシデント調査	ジョージ海峡上空におけるde Havilland DHC-2, N952DBと de Havilland DHC-3, N959PAの空中衝突 (2019)	○	調査当事者向けの情報及びガイダンス
EU	安全調査機関	欧州議会及び欧州理事会の規則(EU) No 996/2010、欧州議会及び欧州理事会の規則(EU) No 376/2014、欧州議会及び欧州理事会の規則(EU) 2018/1139、	—	○	—
英国	航空事故調査局 (AAIB)	欧州議会及び欧州理事会の規則(EU) No 996/2010、民間航空 (航空事故・インシデント調査) 規則 2018、附属書13 航空機の事故とインシデント調査	ロンドン・ガトウィック空港におけるエアバスA321-211型機「G-POWN」の重大インシデント (2020)	—	航空機事故: 救急隊と飛行場運営者のためのガイダンス 航空機事故と重大インシデント: 航空会社向けガイダンス CVR記録検査に関するガイダンス
フランス	航空事故調査局 (BEA)	欧州議会及び欧州理事会の規則(EU) No 996/2010、附属書13 航空機の事故とインシデント調査、運輸法、民間航空法、航空安全調査に関する事前取り決め	Cayenne (Guyane) におけるCessna-207型機 (F-OSIA) の事故	—	—
ドイツ	連邦航空機事故調査局 (BFU)	欧州議会及び欧州理事会の規則(EU) No 996/2010、附属書13 航空機の事故とインシデント調査、航空交通規制、民間航空機運用における事故・インシデントの調査に関する法律	GranseeにおけるCessna-208型機 (Caravan) の事故 (2019)	—	—
エストニア	安全調査センター (OJK)	欧州議会及び欧州理事会の規則(EU) No 996/2010、附属書13 航空機の事故とインシデント調査、航空交通規制航空法、安全調査手順、安全調査センター規程	A320-214 滑走路衝突 (2018)	—	—

【凡例】○:あり / -:なし(公開情報ベース)

2.3 航空分野 EUにおける航空事故調査のスキーム図



※1:登録国、事業者国、設計国、製造国であった場合
 ※2:司法、民間航空、捜索・救助当局など安全調査に関連する活動に関与する可能性のある当局
 ※3:航空機や航空機機器の製造・整備責任者
 ※4:航空機の運航や要員の訓練責任者
 ※5:担当調査官や加盟国の認定代表者に対する代表アドバイザー
 ※6:これらの機関を通じて設計の証明書保有者、製造者や関係する運航者にもコメントを要求する

2.4 自動車分野

自動車分野では、事故調査におけるサイバーを含めた法制度の整備が進んでいない。
EU、英国、ドイツ、エストニアでは、事故調査に関連して安全調査を行う機関が確認できなかった。

国	組織名	関連する法制度	事件事例	サイバーに関する言及	備考(ガイドライン等)
米国	国家運輸安全委員会 (NTSB)	独立安全委員会法、 連邦規則	中型バスの車道からの離脱・リターン・横転 (2019)	—	調査当事者向けの情報及びガイダンス
EU	—	—	—	—	—
英国	—	—	—	—	—
フランス	陸上交通事故調査局 (BEA-TT)	運輸法	大型車両通過時の道路橋の崩壊 (2019)	—	—
ドイツ	—	—	—	—	—
エストニア	—	—	—	—	—

【凡例】—:なし(公開情報ベース)

3. 国内における重要インフラ・産業基盤の各業界における「事故調査」のしくみの調査

- 3.1 国内調査結果サマリー
- 3.2 電力分野
- 3.3 鉄道分野
- 3.4 航空分野
- 3.5 自動車分野
- 3.6 自動車部品分野
- 3.7 鉄鋼分野
- 3.8 建築分野

3.1 国内調査結果サマリー

国内では、事故調査におけるサイバーを含めた法制度の整備が進んでいない。
事故事例についても、サイバーに関連した事故調査が行われたものはない。

分野	組織名	関連する法制度	事故事例	サイバーに関する言及	備考(ガイドライン等)
電力	経済産業省	電気事業法	福島第一原子力発電所事故(2011)	—	—
	原子力規制委員会	原子力規制委員会設置法			
鉄道	運輸安全委員会(JTSB)	運輸安全委員会設置法	金沢シーサイドライン 新杉田駅構内 鉄道人身傷害事故(2019)	—	—
		運輸安全委員会設置法試行規則 事故等調査実施要領通則			
航空	運輸安全委員会(JTSB)	運輸安全委員会設置法	機体の動揺による客室乗務員の負傷(2020)	—	—
		附属書13 航空機の事故とインシデント調査 運輸安全委員会設置法試行規則 事故等調査実施要領通則			
自動車	交通事故総合分析センター(ITARDA)	道路交通法	大型トラックの踏切事故(2019)	—	自工会/部工会・サイバーセキュリティガイドライン V1.0[15]
	事業用自動車事故調査委員会				
自動車部品	交通安全環境研究所	道路運送車両法	乗用自動車の火災(2019)	—	—
鉄鋼	労働災害調査分析センター	労働安全衛生法	合金鉄工場における高温物死亡災害	—	—
建築	昇降機等事故調査部会 消防研究センター	国土交通省組織規則	栃木県内エレベーター事故調査報告書(2012)	—	—
			京都府京都市内油圧エレベーター事故(2019) 静岡工場火災事故(2020)		

【凡例】—:なし(公開情報ベース)

3.2 電力分野

電力分野の事故報告スキームには、電気事業法に基づく「電気事故報告」と、原子力規制委員会設置法に基づく「原子力事故報告」がある。

大手電力事業者においては、サイバー事故調査に対応する体制が整いつつある。

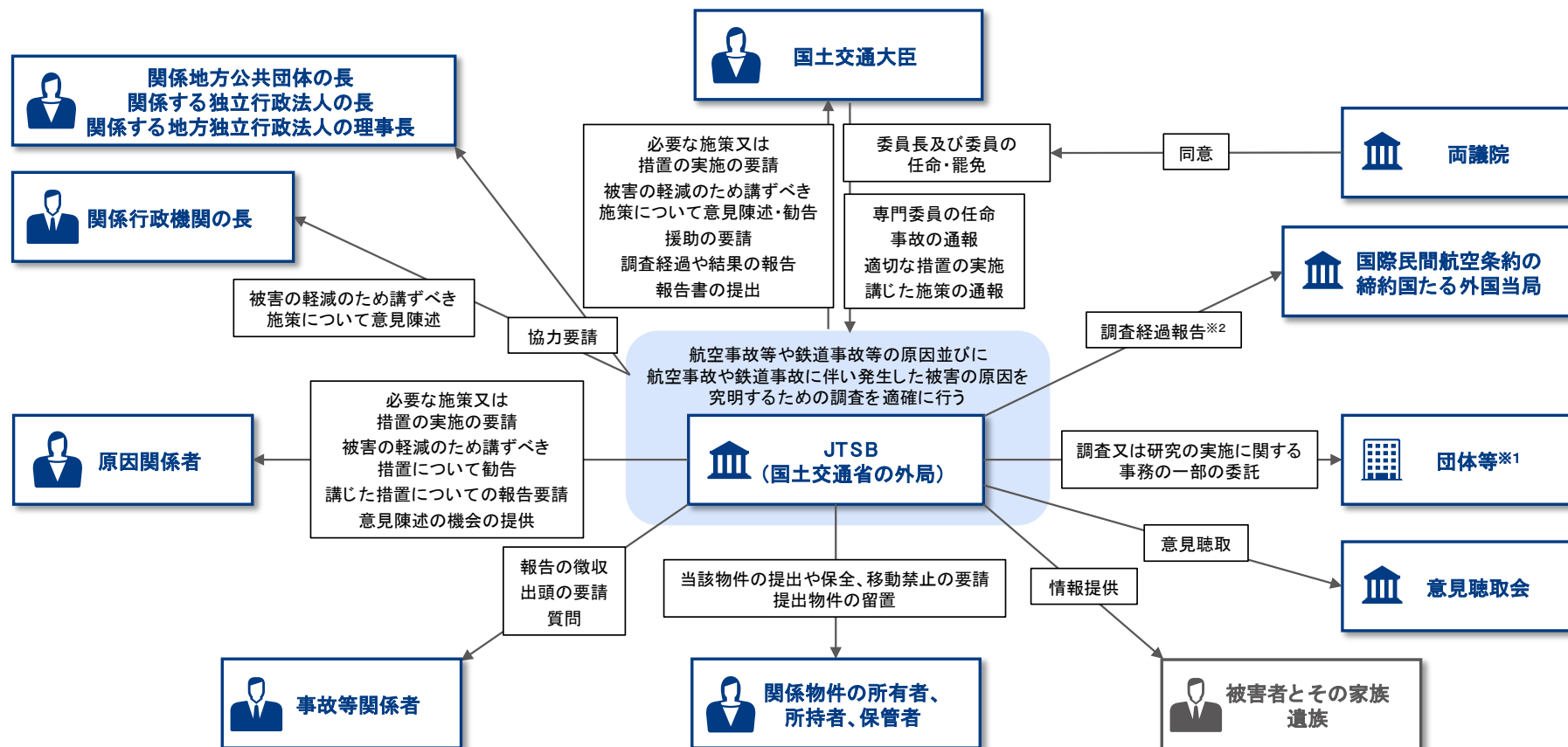


出所) 経済産業省HP 「詳報作成支援システム」より転載。

図 電気事故報告のための「詳報作成支援システム」の概要

3.3 鉄道分野

鉄道分野では、運輸安全委員会設置法に基づき、運輸安全委員会 (JTSCB) による事故調査が行われている。



※1: 独立行政法人、一般社団法人若しくは一般財団法人、事業者その他の民間の団体又は学識経験を有する者

※2: 同条約の規定並びに同条約の附属書として採択された標準、方式及び手続に準拠して航空事故等に関する調査を行う権限を有するものからの要請に基づき、当該当局が行う航空事故等に関する調査の一部として行うものを行う場合

図 JTSCBの事故調査スキーム図



3.4 航空分野

航空分野では、鉄道分野と同じく、運輸安全委員会設置法に基づき、運輸安全委員会 (JTSCB) による事故調査が行われている。

調査スキームは鉄道分野と大きな違いはないが、外国当局との連携に関しても、運輸安全委員会設置法に規定されている。

3.5 自動車分野

自動車分野には、安全目的の事故調査として、交通事故調査分析センターによる調査と、事業用事故調査委員会による調査がある。

道路交通法で規定されている交通事故調査分析センターとして、公益財団法人交通事故総合分析センター (ITARDA) が指定されている。

事業用事故調査委員会は、国土交通省所管の委員会として2014年に設置された(事務局はITARDA)。日本自動車工業会(JAMA)、日本自動車部品工業会(JAPIA)が、共同で「自工会/部工会・サイバーセキュリティガイドライン」を策定している。この中で、事故発生時のサイバー対応について言及されている。

3.6 自動車部品分野

自動車部品分野では、自動車部品に関する安全にかかわる技術的な検証のスキームを確認した。

国土交通省所管の独立行政法人自動車技術総合機構の交通安全環境研究所 (NTSEL) では、国が行う自動車等の基準策定に関する試験研究や提案を行っており、自動車の設計から使用段階まで総合的に対応している。

NTSELのリコール技術検証部では、道路運送車両法の規定に基づき、国土交通省からの依頼により、自動車の構造や装置、性能などが保安基準に適合していない可能性がある場合に、その原因が設計や製作の過程にあるかどうかについて、技術的な検証を行っている。

国内で発生する交通事故や車両火災において車両不具合が疑われる場合は、必要に応じて現地に出張し、事故車両を調査している。さらに、不具合が生じている同型部品や車両を用いて、必要な検証実験を交通安全環境研究所内の施設で行っている。これらの分析調査や検証実験の結果は総合的に検証され、明らかとなった不具合の原因は国土交通省に報告される。



3.7 鉄鋼分野

鉄鋼分野では、工場で発生する事故のうち、主に労働災害に関する事故調査のスキームを確認した。

労働災害調査分析センターでは、厚生労働省所管の独立行政法人労働者健康安全機構の労働安全衛生総合研究所の使命の一つである労働災害の原因究明のための専門的な調査等を行っている。

具体的には、大規模な労働災害や発生メカニズムが複雑な労働災害等について、厚生労働省から災害原因究明の要請等を受けた場合に、各研究グループと連携して、高度な科学的・専門的知見に基づいた原因調査を行っており、その中では、災害発生現場での現地調査や試料の分析、再現実験や数値解析等を実施している。

これらの調査結果は、厚生労働省において、労働安全衛生関係法令の制定や改正、各種技術基準の策定、同種災害の再発防止の指導等を行う際に活用されている。

労働安全衛生法では、労働者健康安全機構による労働災害の原因調査の実施について定められているほか、事業者に求められることについても規定されている。

具体的には、事業者は、政令で定める規模の事業場ごとに、厚生労働省令で定めるところにより、総括安全衛生管理者を選任し、その者に労働災害の原因の調査及び再発防止対策に関する業務を統括管理させなければならないことが記されている。

3.8 建築分野

建築分野では、事故調査の一例として、昇降機事故調査及び火災原因調査のスキームを確認した。

国土交通省の社会資本整備審議会昇降機等事故調査部会では、昇降機及び遊戯施設等に関する事故情報・不具合情報の分析、事故再発防止の観点から、事故発生原因解明に係る調査、事故再発防止対策等に係る調査・検討・意見具申を実施している。

昇降機等の事故調査については、国土交通省組織規則で規定されており、建築指導課に、昇降機等事故対策官を一人設置することが定められている。

火災の原因究明は全国の消防機関の役割であるが、消防機関から要請があった場合や消防庁長官が特に必要があると認めた場合は、消防庁長官による火災原因調査を行えることが消防法で規定されている。

この火災原因調査は、火災種別に応じて消防庁の職員により編成される調査チームが、消防機関と連携して実施する。また、消防庁消防大学校の消防研究センターがその実務を担っている。

調査から得られた知見は必要に応じ、消防行政の施策に反映されている。

4. 「サイバーインシデントに係る事故調査」機能の整備に向けた検討事項

- 4.1 事故調査機能に求められる体制、リソースに関する検討
- 4.2 国内の各分野の特性に応じた対応の検討分野

4.1 事故調査機能に求められる体制、リソースに関する検討

サイバーインシデントに係る事故調査の体制を考える場合、下表の要素による違いを考慮に入れる必要がある。

考慮すべき要素	該当する活動、分野、組織の違い
事故調査のフェーズ	事故発生前: <ul style="list-style-type: none"> 事故調査に必要な情報(国内外のインシデント事例、製品などの脆弱性情報、など)の収集 事故時にサイバー調査が実施可能な人材の育成 事故調査が実施可能な体制の構築
	事故発生時: <ul style="list-style-type: none"> 復旧に向けた緊急対応の支援・助言
	事故発生後: <ul style="list-style-type: none"> 復旧後の原因究明、再発防止対応の支援
対象分野	分野別ISACなどの体制が確立し、サイバーセキュリティ対策に対する体制が整っている分野(例:電力、鉄道、航空)
	分野別ISACなどの体制が立ち上がり、サイバーセキュリティ対策に対する体制が整いつつある分野(例:自動車、自動車部品)
	分野別ISACなどの体制が未確立で、サイバーセキュリティ対策に対する体制が整っていない分野(例:鉄鋼、建築)
対象組織	自組織で事故調査が完結できる組織(大企業、サイバーセキュリティ対策が進んでいる組織)復旧後の原因究明
	自組織のみでは事故調査が十分に実施できない組織(中小企業)

4.1 事故調査機能に求められる体制、リソースに関する検討

事故調査のフェーズごとに、想定される活動、提供する支援機能、必要な能力(ヒト)、必要な設備(モノ)、今後検討が必要な事項を下表に示す。

フェーズ	想定される活動	提供する支援機能	必要な能力(ヒト)	必要な設備(モノ)	今後検討が必要な事項
事故発生前	<ul style="list-style-type: none"> 事故調査に必要な情報(国内外のインシデント事例、製品などの脆弱性情報、など)の収集 	<ul style="list-style-type: none"> インシデントレポート発行 脆弱性情報の提供 	<ul style="list-style-type: none"> 情報収集 	<ul style="list-style-type: none"> 機密性の高い情報を管理する設備 	<ul style="list-style-type: none"> 既存の国等の取り組みとの差別化 事故調査に特化した情報収集の要否
	<ul style="list-style-type: none"> 事故時にサイバー調査が実施可能な人材の育成 事故調査が実施可能な体制の構築 	<ul style="list-style-type: none"> 人材教育プログラムの提供 組織内の事故調査体制構築支援プログラムの提供 	<ul style="list-style-type: none"> 教育プログラムの企画、開発 教育プログラムの実施 体制構築支援プログラムの提供 	<ul style="list-style-type: none"> 教育施設 教育プログラム 	<ul style="list-style-type: none"> 事故調査に適した教育プログラムの開発 事故調査が実施可能な体制構築(組織内体制、ファシリティ、予算確保、判断基準、対策実施基準、など)に向けた支援内容の検討
事故発生時	<ul style="list-style-type: none"> 復旧に向けた緊急対応の支援・助言 	<ul style="list-style-type: none"> 現場での緊急対応支援 報告窓口の一元化 関連する情報提供 	<ul style="list-style-type: none"> インシデント調査 報告窓口 情報提供 	<ul style="list-style-type: none"> インシデント調査に必要な機材 報告情報管理機能 	<ul style="list-style-type: none"> 突発的に発生する様々な分野のインシデントに対応できる人材の常時確保の要否 窓口一元化の要否
事故発生後	<ul style="list-style-type: none"> 復旧後の原因究明 	<ul style="list-style-type: none"> フォレンジック支援 	<ul style="list-style-type: none"> フォレンジック調査 	<ul style="list-style-type: none"> フォレンジックに必要な機材 	<ul style="list-style-type: none"> 分野ごと、組織ごとに異なるシステムに対する支援を実施可能な体制の確保 被害状況の公開、企業の免責に関する検討
	<ul style="list-style-type: none"> 再発防止対策の支援 	<ul style="list-style-type: none"> サイバーセキュリティ対策検討支援 	<ul style="list-style-type: none"> サイバーセキュリティ対策検討 	<ul style="list-style-type: none"> サイバーセキュリティ対策の検討に必要な機材 	

4.2 国内の各分野の特性に応じた対応の検討分野

前頁の表中の「必要な能力(ヒト)」及び「必要な設備(モノ)」を整理すると、「情報収集・提供」、「インシデント対応」、「フォレンジック対応」、「人材育成・体制構築支援」の4つの機能に大別できる。

この4機能の要否について、対象分野・対象組織の違いから検討した。

		分野① 分野別ISACなどの体制が確立し、サイバーセキュリティ対策に対する体制が整っている分野 (例:電力、鉄道、航空)	分野② 分野別ISACなどの体制が立ち上がり、サイバーセキュリティ対策に対する体制が整いつつある分野 (例:自動車、自動車部品)	分野③ 分野別ISACなどの体制が未確立で、サイバーセキュリティ対策に対する体制が整っていない分野(例:鉄鋼、建築)
自組織で事故調査が完結できる組織 (大企業、サイバーセキュリティ対策が進んでいる組織)	情報収集・提供	<ul style="list-style-type: none"> ISAC等既存の活動があるため、「情報収集・提供」へのニーズは低い。 他分野の情報は不足していると考えられる。 		<ul style="list-style-type: none"> 「情報収集・提供」へのニーズは高い。
	インシデント対応	<ul style="list-style-type: none"> 突発的に発生するインシデント発生直後の直接的な支援は、体制面で困難と考えられる。 		
	フォレンジック対応	<ul style="list-style-type: none"> 自社人材や外部リソースにより自力でインシデント対応が可能のため、「フォレンジック対応」へのニーズが低い。 		<ul style="list-style-type: none"> 自社人材が不足しており、「フォレンジック対応」へのニーズが高い。
	人材育成・体制構築支援	<ul style="list-style-type: none"> 自社人材の育成について、「人材育成」へのニーズが高い。 事故調査体制は、すでに構築済みか、今後自力で構築が可能。 		
自組織のみでは事故調査が十分に実施できない組織 (中小企業)	情報収集・提供	<ul style="list-style-type: none"> ISAC等既存の活動があるため、「情報収集・提供」へのニーズは低い。 他分野の情報は不足していると考えられる。 		<ul style="list-style-type: none"> 「情報収集・提供」へのニーズは高い。
	インシデント対応	<ul style="list-style-type: none"> 突発的に発生するインシデント発生直後の直接的な支援は、体制面で困難と考えられる。 		
	フォレンジック対応	<ul style="list-style-type: none"> 自社人材が不足しており、「フォレンジック対応」へのニーズが高い。 		
	人材育成・体制構築支援	<ul style="list-style-type: none"> 自社人材の育成ニーズはありつつ、必要な人材を自社内で確保することが難しいため、「人材育成」へのニーズは不透明。外部リソースを活用できる人材等、必要な人材像やかかけられるコストについて検討が必要。 事故調査体制は未整備で、自力での構築が難しい。サイバー調査に向けた組織体制の在り方、ログ取得などのファシリティ整備、必要な予算の確保、サイバー攻撃の有無を判断する基準の整備、などの各種支援に向けた検討が必要。 		