3．重要インフラ等におけるサイバーセキュリティの確保

令和元年度に評価対象とした「重要インフラ等におけるサイバーセキュリティの確保」についても、平成 30 年度に実施した 10 課題最終評価と同様に「概要」と「評価」の 2 つの部分から構成している。

「概要」では、研究開発計画等を基にして背景と目的、実施体制、予算、研究開発テーマ、出口戦略、ロジックツリーについて整理している。

「評価」では、課題評価アンケート調査（研究責任者向け）と課題評価インタビュー調査（研究責任者向け）の結果も踏まえつつ、PD による自己点検報告等に基づく課題評価 WG での評価結果をベースに、表 2-10 に示した評価項目の大項目別に取りまとめている。

(1)意義の重要性、SIP の制度の目的との整合性	● 我が国の重要インフラ等の安定運用に貢献するとともに、我が国の機器やシステムの市場競争力を高め、さらにはインフラ産業の国際競争力向上にも貢献することが期待できる。 ● サイバーセキュリティ技術のユーザーとなる重要インフラ等事業者と密に協議する体制を実現できたため、重要インフラ等事業者がサイバーセキュリティ技術を導入するに際してのニーズを的確にフィードバックできた。 ● サイバーセキュリティ技術を有する複数企業が得意領域を基に研究テーマを分担し、また各社の重要インフラ等事業者とのネットワークを互いに共有できたため、効率的・有効な研究開発ができた。 ● 省庁連携が実現されたことで、複数分野の重要インフラ等における展開を効果的・有効に実行できた。
(2)目標・計画・戦略の妥当性	● サイバーセキュリティ技術を重要インフラ等に実装し、オリパラに貢献することを掲げる目標は多様なステークホルダーが問題意識を共有し、一丸となることができる適切な設定だった。 ● 計画は、PD によりコア要素技術から社会実装まで、体系的に設定されていた。
(3)課題におけるマネジメント（適切なマネジメントがなされているか。）	● PD による強力で細やかなリーダーシップ、重要インフラ等事業者を巻き込んだ推進委員会・WG により適切なマネジメントの下で各研究開発テーマ内実施者間連携、重要インフラ等事業者等との関係が構築され、有効に機能した。
(4)直接的な研究成果（アウトプット）	● 真贋判定技術は 1 台あたり数十万の大量ファイルからなる、数百～数千台レベルのサーバ機器に対応し大規模システム全体の監視を実現した。 ● 動作監視・解析のコア技術となる「収集・蓄積・分析技術」「IoT-ゲートウェイと深層学習による監視・分析技術」「制御 NW センサ技術及び統合解析技術」を確立した。 ● ログ分析・バックドア解析、モデル解析の結果を、同一インフラ事業者間や、内容によってはインフラ分野をまたいで情報を

	安全に共有する機能を実現する情報共有プラットフォーム技術を開発した。 ● 重要インフラ等における OT（制御技術）運用者がサイバーセキュリティの方策検討やインシデント対応等を適切に実施するための講義・演習教材やシステムを開発した。
(5)現在・将来の波及効果（アウトカム）	● 本課題の成果は国内のインフラ産業（180 兆円規模）の安定運用に貢献することが期待されている。また、重要インフラ等向けセキュリティ製品市場の新規創出が見込まれている。 ● 「先行版」として首都圏近郊の主要インフラに社会実装が実施されており、2020 年開催東京オリンピック・パラリンピック競技大会のサイバーセキュリティ確保が期待されている。国内での実績がインフラ輸出へつながることが期待される。 ● 動作監視・解析技術は「制御 NW センサ技術及び統合解析技術」と協力して製品開発を行い、日立製作所が HAD（Hitachi Anomaly Detector）として 2017 年に製品化した。 ● 情報共有プラットフォーム技術は日立システムズ社が国際標準 STIX/TAXII 準拠の国内事業者向けサービス「SHIELD」として 2018 年に商用化している。 ● セキュリティ教育カリキュラム・講義・演習教材・e-learning 環境を開発した。教材は既に 40 を超える組織（電事連、NTT-ME、日立等多数）に配布され、人材育成を推進している。
(6)改善すべきであった点と今後取り組むべき点	● SIP のような外部有識者を評価者として予算配分を決定するような技術開発に関して、その取り組みや成果についてどのように開示することが適切かは課題であった。 ● SIP 第 1 期終了後も、セキュリティ技術を有する事業者と重要インフラ事業者の間で、維持管理や残課題等について検討を継続していく必要がある。また人材育成についても継続的な検討が必要である。 ● 今回の成果を拡（ひろ）げるため、国内重要インフラ等事業者に対して、どのようなインセンティブやルールでサイバーセキュリティ技術を売り込んでいくかについても、ユーザー視点かつ具体的に議論していく必要がある。 ● セキュリティのような分野では事前に関係省庁で出口について協議して、例えば調達要件等も含めて検討するべきである。 ● まずは国内インフラ事業者への導入を進めていくことにより、海外展開として、重要インフラ等とサイバーセキュリティと人材育成（プログラム）をパッケージ化して輸出することにつながると期待される。重要インフラ等事業者への導入状況、国際的な具体的な方針の検討状況について、内閣府による追跡的なフォロー及び評価・フィードバックが必要である。

3.1 概要

3.1.1 背景と目的

2020 年東京オリンピック・パラリンピック競技大会を迎える我が国にとって、サイバー攻撃の脅威は切実な問題であり、強固なサイバーセキュリティの確保による世界で最も安心・安全な社会基盤の確立が必達の課題である。

本課題では、重要インフラ[1]等におけるサイバーセキュリティを確保するために、重要インフラ等サービスの安定運用を担う制御ネットワーク及び制御ネットワークを構成する制御・通信機器（以下「制御・通信機器」という。）のサイバー攻撃対策として、制御・通信機器のセキュリティ確認[2]技術、制御・通信機器及び制御ネットワークの動作監視・解析技術と防御技術を研究開発した。特に、「通信・放送」「エネルギー」「交通」分野を重点領域とした。

その成果を、2020 年東京オリンピック・パラリンピック競技大会をターゲットに、実証実験等を通して、通信・放送、エネルギー、交通などのインフラシステムに適用できることを確認した。また、今後普及・拡大が見込まれる IoT システムのセキュリティ確保に向けて前記技術を拡張するとともに、技術導入を支援する適合性確認の在り方と仕組みの検討、分野を超えた運用のための共通プラットフォームの実現、セキュリティ人材育成に取り組んだ。

3.1.2 実施体制

令和元年度時点で、サブ PD は 1 名、研究責任者は 11 名である。管理法人は、新エネルギー・産業技術総合開発機構（NEDO）となっている。

研究開発テーマは研究開発(a1)～(a4)のコア技術と、その出口となる社会システムにおいて実装する(b1)～(b5)の社会実装技術とし、それらを密に連携して進めた。

---

[1] 「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」が特定している 14 分野に代表される重要な社会基盤システム。

[2] セキュリティ確認とは、機器やソフトウェアの真正性、完全性を確かめること。

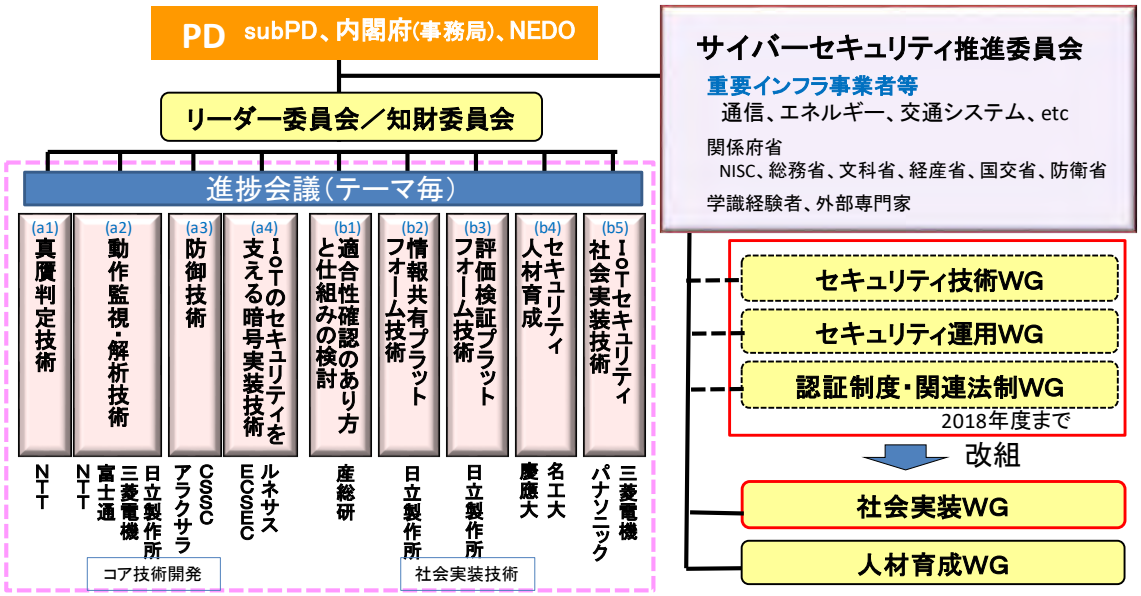

図 3-1　重要インフラ等におけるサイバーセキュリティの確保の研究体制

（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

表 3-1　重要インフラ等におけるサイバーセキュリティの確保の PD 等

区分	所属	氏名
PD	情報セキュリティ大学院大学学長	後藤　厚宏
サブ PD	慶應義塾大学環境情報学部教授	手塚　悟

令和 2 年 1 月 1 日現在

表 3-2　重要インフラ等におけるサイバーセキュリティの確保の主要会議体

名称	構成員	概要
推進委員会	PD、サブ PD、専門家、関係省庁、事務局（内閣府）、管理法人（NEDO）（表 0-3 参照）	PD が議長、内閣府が事務局を務め、関係府省、管理法人、専門家等が参加する推進委員会を内閣府に置き、当該課題の研究開発計画の作成や実施等に必要な調整等を行う。令和元年度末までに 12 回開催（年 2・3 回程度開催）
知財委員会	PD、サブ PD、内閣府、NEDO、研究責任者	NEDO に置く。各受託機関で出願される知的財産の動向を把握・管理し、産業利用する際の利便性向上につながるよう、各受託機関と調整を行う。（年 6 回程度開催）
リーダー委員会※	PD、サブ PD、内閣府、NEDO、研究責任者	全体的な課題、スケジュールについて共有する。（年 6 回程度開催）

進捗会議※	PD、サブ PD、内閣府、NEDO、関係する研究機関	テーマ毎に設け、研究開発の進捗状況について確認するとともに、課題の解決策・研究方針について PD 等から指導。 （各テーマ年 6 回程度開催）
セキュリティ技術 WG※ （～2018 年度）	PD、サブ PD、株式会社エヌ･ティ･ティエムイー、エヌ･ティ･ティ･コミュニケーションズ株式会社、情報処理推進機構、東京地下鉄株式会社、株式会社 KDDI 総合研究所、東京電力ホールディング株式会社、東日本電信電話株式会社、東日本旅客鉄道株式会社、三菱重工業株式会社、NISC、総務省、経産省、防衛装備庁、研究責任者 神戸大学 NEDO、内閣府	研究開発成果を重要インフラ等事業者の制御・通信システムに導入する上で必要となるセキュリティ要件及びそれに対する課題を検討し、研究開発にフィードバックを行う。 （年 4 回程度開催）
セキュリティ運用 WG※ （～2018 年度）	PD、サブ PD、エヌ・ティ･ティ･コミュニケーションズ株式会社、JPCERT コーディネーションセンター、情報処理推進機構、情報通信研究機構、東京ｵﾘﾝﾋﾟｯｸ・ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会組織委員会、東京地下鉄株式会社、東京電力ホールディングス株式会社、東京都、日本放送協会、日本民間放送連盟、東日本電信電話株式会社、三菱重工業株式会社、NISC、防衛装備庁、研究責任者 明治大学 NEDO、内閣府	重要インフラ等において必要となる横断的情報共有の仕組み及び情報分析機能を検討するとともに、オペレーション全体に関わる課題を検討。情報共有及び連携を実現する上での課題を整理して研究開発にフィードバックを行う。 （年 4 回程度開催）

認証制度・関連法制 WG※ （～2018 年度）	PD、サブ PD、情報処理推進機構、三菱重工業株式会社、NISC、防衛装備庁、研究責任者 慶應義塾大学 NEDO、内閣府	重要インフラ等分野に関する国際標準、既存の各種基準等に関連する制度・組織を調査し、コア技術を社会実装するために必要な要件を整理する。 （年 3 回程度開催）
人材育成 WG※	PD、サブ PD、株式会社エヌ・ティ・ティエムイー、エヌ・ティ・ティ・コミュニケーションズ株式会社、東京地下鉄株式会社、東芝デバイス＆ストレージ株式会社、日本電気株式会社、三菱重工業株式会社、NISC、総務省、経産省、防衛装備庁、研究責任者 東北大学 NEDO、内閣府	重要インフラ等事業者における運用実務において求められるセキュリティ教育、意識について検討し、運用担当者のセキュリティ技術レベルの向上に必要な人材育成方法に関する課題と要件を整理して研究開発にフィードバックを行う。 （年 3 回程度開催）

社会実装 WG※ （2019 年度）	PD、サブ PD、ICT-ISAC、株式会社エヌ・ティ・ティエムイー、エヌ・ティ・ティ・コミュニケーションズ株式会社、株式会社 KDDI 総合研究所、静岡大学、情報通信研究機構、情報処理推進機構、JPCERT コーディネーションセンター、東京ｵﾘﾝﾋﾟｯｸ・ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会組織委員会、東京電力ホールディングス株式会社、東京地下鉄株式会社、鉄道総合技術研究所、東芝デバイス＆ストレージ株式会社、日本民間放送連盟、東日本電信電話株式会社、三菱重工業株式会社、NISC、総務省、経産省、防衛装備庁、研究責任者 神戸大学 明治大学 NEDO、内閣府	開発した技術に関して技術・運用等の観点を考慮し、現在協働検討体制を構築して推進している事業者だけではなく、幅広い分野へ社会実装(横展開)を実現するための方策を議論。 （年 3 回程度開催）

※本課題に特徴的な会議体。

表 3-3　重要インフラ等におけるサイバーセキュリティの確保推進委員会 構成員一覧表

区分	所属	氏名
PD	情報セキュリティ大学院大学学長	後藤　厚宏
サブ PD	慶應義塾大学環境情報学部教授	手塚　悟
専門家	一般社団法人 JPCERT コーディネーションセンター常務理事	有村　浩一
	情報処理推進機構セキュリティセンター長	瓜生　和久
	東日本旅客鉄道株式会社常務執行役員	大内　敦
	MHI エアロスペースシステムズ株式会社常務取締役	大島　健二
	電気事業連合会情報通信部長	大友　洋一
	トヨタ自動車株式会社　先進技術開発カンパニーフェロー（SIP 自動走行システム PD）	葛巻　清吾
	情報通信研究機構サイバーセキュリティ研究所長	久保田　実

	東京電力ホールディングス株式会社常務執行役	関　知道
	東北大学サイバーサイエンスセンター教授	曽根　秀昭
	公益財団法人東京ｵﾘﾝﾋﾟｯｸ･ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会組織委員会テクノロジーサービス局長	舘　剛司
	株式会社 KDDI 総合研究所取締役執行役員副所長	田中　俊昭
	東京地下鉄株式会社取締役	中澤　英樹
	明治大学経営学部経営学科教授	中西　晶
	東京都戦略政策情報推進本部情報基盤担当部長	沼田　文彦
	東日本電信電話株式会社取締役ネットワーク事業推進本部設備企画部長	星野　理彰
	日本放送協会情報システム局 CSIRT 部専任部長	溝渕　俊憲
	神戸大学大学院工学研究科電気電子工学専攻教授	森井　昌克
	一般社団法人日本民間放送連盟事務局長兼総務部長	渡辺　昌己
関係省庁	内閣官房内閣サイバーセキュリティセンター内閣参事官	上田　光幸
	内閣官房内閣サイバーセキュリティセンター内閣参事官	結城　則尚
	総務省サイバーセキュリティ統括官付参事官	大森　一顕
	文部科学省研究振興局参事官	橋爪　淳
	経済産業省商務情報政策局サイバーセキュリティ課長	奥家　敏和
	国土交通省総合政策局情報政策課サイバーセキュリティ対策室長	大嶋　孝友
	国土交通省鉄道局総務課危機管理室長	野本　英伸
	防衛装備庁技術戦略部技術戦略課長	堀江　和宏
事務局	内閣府大臣官房審議官（科学技術・イノベーション担当）	髙原　勇
	内閣府政策統括官（科学技術・イノベーション担当）付参事官	近藤　玲子
	内閣府政策統括官（科学技術・イノベーション担当）付政策調査員	岡崎　皓広
管理法人	新エネルギー・産業技術総合開発機構 IoT 推進部長	安田　篤

令和元年 12 月 13 日（開催日）現在

3.1.3　予算

表 3-4　重要インフラ等におけるサイバーセキュリティの確保の予算

年度	予算（億円）
平成 27（2015）年度	5.0
平成 28（2016）年度	25.5
平成 29（2017）年度	27.1
平成 30（2018）年度	23.0
令和元（2019）年度	18.4
合計	99.0

3.1.4　研究開発テーマ

本課題では、重要インフラ[3]等におけるサイバーセキュリティを確保するために、重要インフラ等サービスの安定運用を担う制御ネットワーク及び制御ネットワークを構成する制御・通信機器（以下「制御・通信機器」という。）のサイバー攻撃対策として、制御・通信機器のセキュリティ確認[4]技術、制御・通信機器及び制御ネットワークの動作監視・解析技術と防御技術を開発した。そして、2020 年東京オリンピック・パラリンピック競技大会をターゲットに、実証実験等を通して、その成果を通信・放送、エネルギー、交通などのインフラシステムに適用できることを確認した。また、今後普及・拡大が見込まれる IoT システムのセキュリティ確保に向けて前記技術を拡張するとともに、技術導入を支援する適合性確認の在り方と仕組みの検討、分野を超えた運用のための共通プラットフォームの実現、セキュリティ人材育成にも取り組んだ。

本課題の研究開発テーマは図 3-2 の通り研究開発に関する a と社会実装に関する b の 2 つに大別されている。

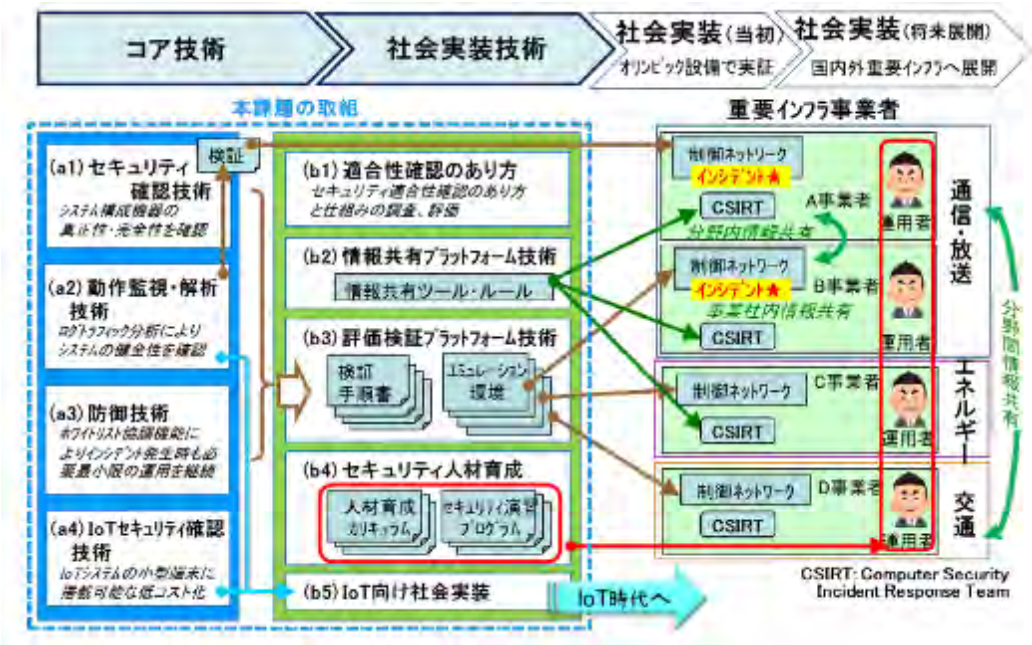

図 3-2　研究開発計画の全体像

（出典）内閣府　政策統括官（科学技術・イノベーション担当）「戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保　研究開発計画（令和元年 7 月 11 日）」（令和 2 年 1 月閲覧）<https://www8.cao.go.jp/cstp/gaiyo/sip/keikaku/11_cyber.pdf>

[3] 「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」が特定している 14 分野に代表される重要な社会基盤システム。

[4] セキュリティ確認とは、機器やソフトウェアの真正性、完全性を確かめること。

a. 制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

「システムの免疫力」の向上につながるコア技術の研究開発を行った。

(a1) 制御・通信機器のセキュリティ確認技術

本研究開発テーマでは、機器の製造に組み込まれる不正機能の混入を想定したセキュリティ機能により、システム構築時とシステム運用時に制御・通信機器のセキュリティ（真正性・完全性）確認ができ、その確認結果を理論的、又は実用的に担保可能な技術を開発した。

表 3-5　制御・通信機器のセキュリティ確認技術に関する研究体制

研究開発実施機関 （計 1 機関）	日本電信電話株式会社

(a2) 制御・通信機器および制御ネットワークの動作監視・解析技術

本研究開発テーマでは、システムの運用時に、システムとして健全な状態であることを確認するために制御・通信機器および制御ネットワークに対する効率的なログ収集、ログ解析による動作監視、さらには、バックドア解析、重要インフラ等分野で共通化可能な知識の解析モデル等の先端的な機能を開発した。

表 3-6　制御・通信機器および制御ネットワークの動作監視・解析技術に関する研究体制

研究開発実施機関 （計 4 機関）	日本電信電話株式会社、富士通株式会社、三菱電機株式会社、株式会社日立製作所

(a3) 制御・通信機器およびシステムの防御技術

本研究開発テーマでは、制御・通信機器の状態を監視し、機器の異常を検知した場合、制御システムの可用性を重視し、安全な機器のみで処理を継続するホワイトリスト協調技術を開発した。

表 3-7　制御・通信機器およびシステムの防御技術に関する研究体制

研究開発実施機関 （計 2 機関）	アラクサラネットワークス株式会社（2018 年度～） 技術研究組合制御システムセキュリティセンター

(a4) IoT 向けセキュリティ確認技術

本研究開発テーマでは、高信頼な暗号処理や通信により IoT 機器の成り済ましおよびセンシングデータの改ざんを防止する技術、IoT 機器上のソフトウェアの真正性・完全性を確認する技術、製造段階での不正機能を確認する機器テスト技術を開発した。

表 3-8　IoT 向けセキュリティ確認技術に関する研究体制

研究開発実施機関 （計 2 機関）	電子商取引安全技術研究組合、ルネサスエレクトロニクス株式会社

b. 社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

「組織対応能力」向上」につながる社会実装技術の研究開発を行った。

(b1) 研究開発技術の社会実装を促す適合性確認のあり方

本研究開発テーマでは、重要インフラ等システムの制御ネットワークや政府系システム、およびその制御・通信機器の製造者とその機器等を想定し、セキュリティ適合性確認のあり方と仕組みを調査、評価した。

表 3-9　研究開発技術の社会実装を促す適合性確認のあり方に関する研究体制

研究開発実施機関 （計 1 機関）	産業技術総合研究所

(b2) 情報共有プラットフォーム技術

本研究開発テーマでは、ログ分析・バックドア解析、モデル解析の結果を、発見された情報の緊急性や普遍性等に応じ、営業秘密等にも配慮しながら、同一インフラ事業者間や、内容によってはインフラ分野をまたいで情報を安全に共有する機能を実現した。

表 3-10　情報共有プラットフォーム技術に関する研究体制

研究開発実施機関 （計 1 機関）	株式会社日立製作所

(b3) 評価検証プラットフォーム技術

本研究開発テーマでは、エネルギー系・交通系事業者のシステムに(a2)技術を早期に適用するための評価手順、検証環境等を整備し、評価検証を実施した。また、重要インフラ等システムに広く本技術を適用するための検討も行った。

表 3-11　評価検証プラットフォーム技術に関する研究体制

研究開発実施機関 （計 2 機関）	株式会社日立製作所 NTT コミュニケーションズ株式会社（2017 年度まで）

(b4) セキュリティ人材育成

本研究開発テーマでは、(b4-1) OT（制御技術）運用者のセキュリティ技術を向上するための人材育成のフレームワーク、カリキュラム、OJT による実践的教育の設計を実施した。

表 3-12　セキュリティ人材育成(b4-1)に関する研究体制

研究開発実施機関 （計 1 機関）	慶應義塾大学

また、(b4-2)電気、ガス、石油、化学プロセス等の重要インフラ等におけるセキュリティインシデント発生時の対応能力向上のための演習を開発し、試用した。

表 3-13　セキュリティ人材育成(b4-2)に関する研究体制

研究開発実施機関 （計 1 機関）	名古屋工業大学

(b5) IoT セキュリティ社会実装技術

本研究開発テーマでは、(b5-1)IoT 向けセキュリティ対策技術の社会実装を促進するため、IoT セキュリティに求められる技術、社会実装のための協業体制、IoT システムのセキュリティ要件を満足しているかの評価、実運用に必要なセキュリティ人材について課題と要件の調査等を実施した。IoT セキュリティエコシステムの実現に必要な要件と運用体制の構築についても検討を行った。（2018 年度から（a4-2）を本テーマに一体化している。）

表 3-14　IoT セキュリティ社会実装技術(b5-1)に関する研究体制

研究開発実施機関 （計 1 機関）	パナソニック株式会社

また、(b5-2)IoT 機器の動作監視・解析を可能にする IoT 機器向けゲートウェイの社会実装に向け、IoT セキュリティ監視サービスとしての提供を実現すべく、SOC 連携とホワイトリスト型動作監視・解析技術の併用を中心とした調査・検討・評価等を行う。

表 3-15　IoT セキュリティ社会実装技術 (b5-2)に関する研究体制

研究開発実施機関 （計 1 機関）	三菱電機株式会社

3.1.5　研究開発テーマと各省庁施策との連関図

研究開発テーマと各省庁施策との連関図を図 3-3 に示す。

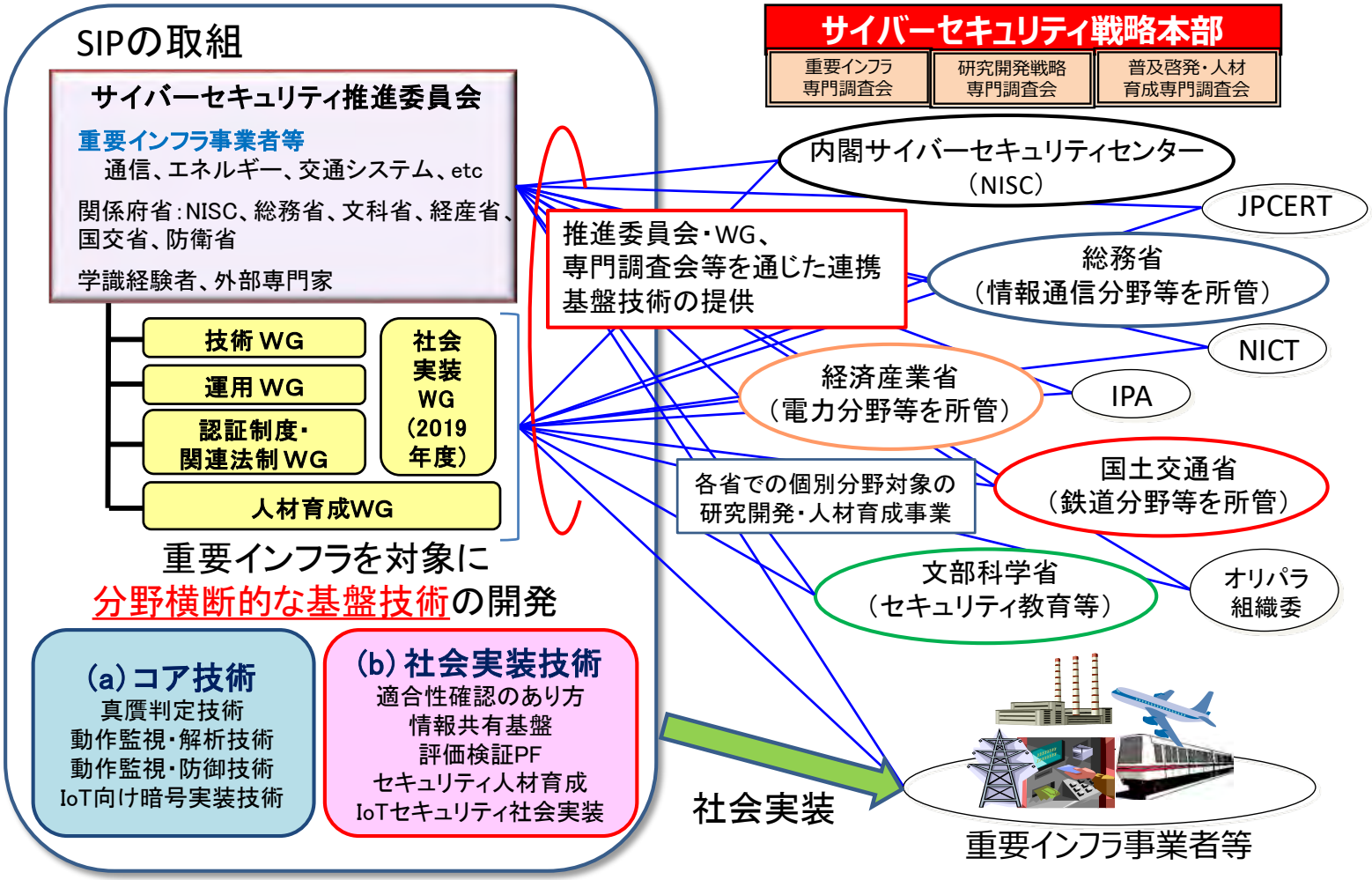

図 3-3　重要インフラ等におけるサイバーセキュリティの確保の研究開発テーマ及び各省庁施策との連関図

3.1.6　出口戦略

(1) 国内インフラ産業への展開と安定運用への貢献

オリパラを契機として重要インフラ等への先行導入や社会実装のための技術開発、人材育成のための基盤整備等を進める。その後は開発成果及びオリパラでの実績を基に重要インフラ等事業者を始め幅広い分野に研究開発の成果を展開し、国内インフラ産業の安定運用へ貢献することを目指す。

(2) 重要インフラ等輸出の国際競争力確保

国内インフラ産業における運用実績を積み、重要インフラ等に係る設備と合わせてインフラシステム全体として海外への展開を図る。現状サイバーセキュリティ対策に関する製品等は海外事業者に大きく依存しているが、開発成果を競争力としたインフラ展開により市場の競争力優位獲得を目指す。

3.1.7　分析フレーム（ロジックツリー）

評価に際して、研究開発活動がもたらす直接的な研究成果と、現在・将来の波及効果について、令和元（2019）年度研究開発計画からロジックツリーにより整理を行った結果を図3-4に示す。

本課題は、コア技術である制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発、社会実装のために必要な共通プラットフォーム実現のための研究開発及びサイバーセキュリティ人材育成を進め、オリパラに向けて重要インフラ等の制御ネットワーク等に先行導入することを短期的な目標として設定している。また、これと並行して研究開発技術を実装した製品・サービスの展開、IoT用の製品開発・成果普及に向けた体制整備、重要インフラ等設備への導入を容易にするガイドライン整備、人材育成のためのコミュニティ形成・教材更新方法の確立についても短期的な目標として設定されている。中長期的には、オリパラでの実績を基に重要インフラ等事業者をはじめとして開発成果が広く導入され、国内インフラ産業の安定運用の貢献とサイバー攻撃による社会的損失の回避が社会的目標として設定されている。加えて、それに伴い重要インフラ等事業者のインシデント対応能力向上等に伴い、重要インフラ等事業者の輸出時における国際競争力が向上することも産業的目標として設定されている。また、重要インフラ向けセキュリティ製品市場の新規創出も産業的目標として設定されている。

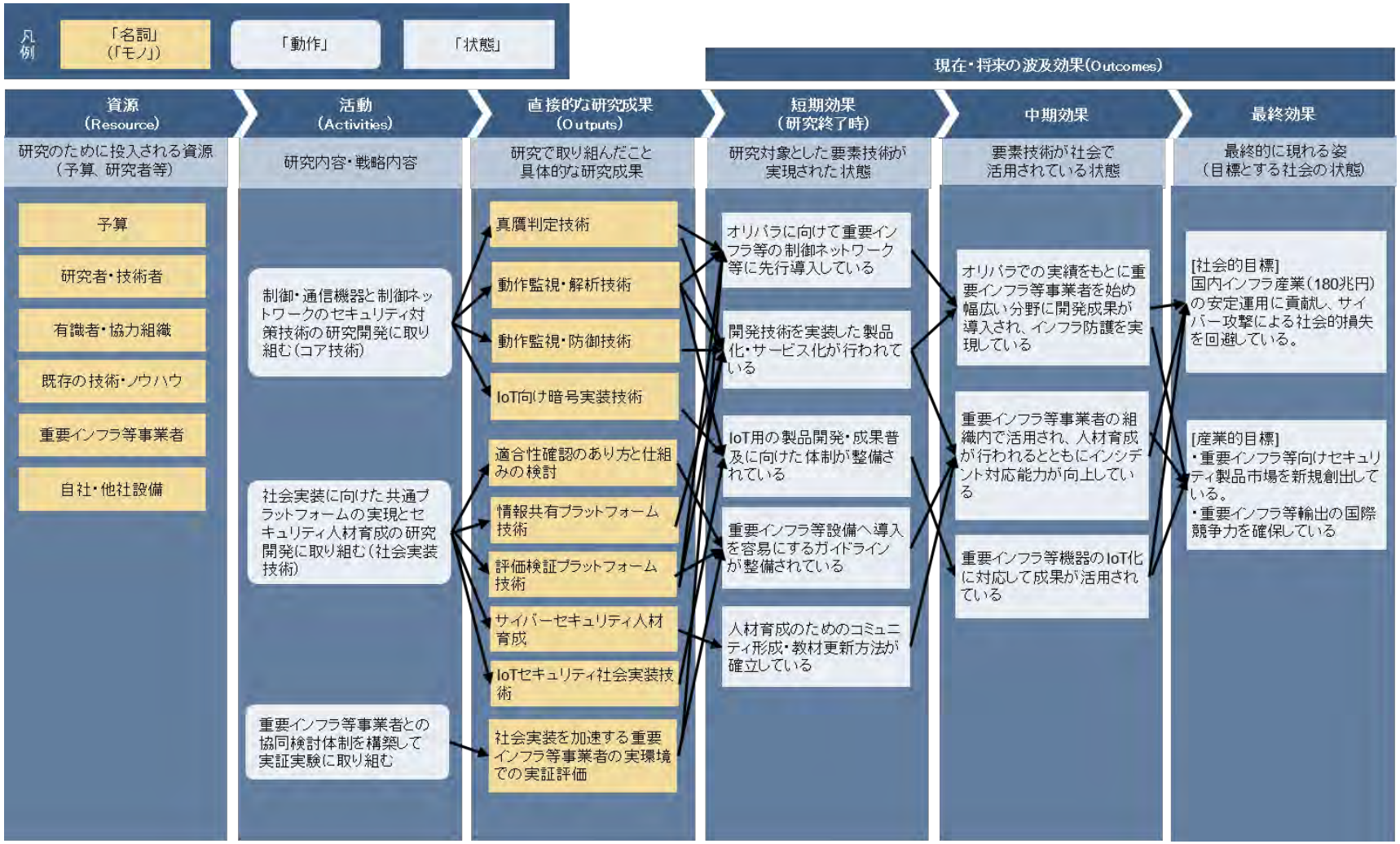

図 3-4　「重要インフラ等におけるサイバーセキュリティの確保」ロジックツリー

（出典）「戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保）研究開発計画」（2019/7/11）を基に作成。