令和７年度
特許出願技術動向調査報告書（要約）
－サイバー攻撃検知技術～不正侵入・マルウェア等の検知に向けた情報セキュリティ技術～－

令和８年３月

特　許　庁

巻頭言

社会のデジタル化の大幅な進展は、情報セキュリティを含むサイバーセキュリティにおける多様で複雑な脅威とそれに伴うリスクへの対応を不可避なものとしている。特許庁は平成27(2015)年度に情報セキュリティ技術全般に関する特許出願技術動向調査を行った。それから10年がたち、サイバーセキュリティを取り巻く状況は大きく変化し、関連する技術分野も大幅に拡大していることを捉え、今般、社会的なインパクトが大きいと見られるサイバー攻撃の検知技術に焦点を当てた特許出願技術動向調査を行うこととなった。

この特許出願技術動向調査においては、侵入検知・マルウェア検知に関する市場環境、特許動向、研究開発動向の調査結果と、有識者からのヒアリングで得た知見を統合的に分析し、我が国の技術開発の現状と今後の方向性につき整理した。また、脅威インテリジェンス及び主要産業向け攻撃検知技術の二つの観点を中心に分析を行った。

得られた主な知見は次のように要約できる。我が国は脅威インテリジェンスに関する特許出願や論文発表数が少なく、国内のサイバーセキュリティ市場も国外ベンダによる製品の寡占が進んでいる。一方、車両、製造装置等の分野は、引き続き我が国が特許出願数で優位性を維持しているものの、他国の出願数増加に伴ってその優位性が揺らぐおそれがある。また、医療及び金融の分野においては一定の成長が見られる。

総合分析においてはこれらに対して、(1)日本国内に脅威インテリジェンスを蓄積する仕組みを整備すること、(2)重要インフラ分野や国際競争力を有する産業向けのサイバー攻撃検知技術の強化に向けて特許出願及び研究開発を進めること、を示唆としてまとめている。

本報告書がサイバーセキュリティにおける我が国の競争力を高めるための一助となり、関係各位の戦略策定や技術投資に資することがあれば誠に幸いである。

末筆ながら、多数の特許文献や論文などの調査分析を担当した調査会社の方々、ヒアリングに協力いただいた企業・団体の方々、及び、調査方法と報告書に対して多大な助言をいただいた各方面の方々に、感謝を申し上げる。

令和７年度特許出願技術動向調査 －サイバー攻撃検知技術
～不正侵入・マルウェア等の検知に向けた情報セキュリティ技術～－
アドバイザリーボード 委員一同

目次

要約

第１章　技術と調査の概要

第１章では、本調査の概要を紹介する。調査の目的、調査対象範囲、調査する技術区分、調査方法について記載する。

第１章の要約

- 本調査の目的は、(1)本テーマにおける国内外の技術発展状況、研究開発状況を含む技術動向を明らかにすること、(2)本テーマにおける日本及び外国の技術競争力、産業競争力を明らかにすること、及び(3)本テーマにおいて日本企業・政府機関が取り組むべき課題を整理し、日本の強み・弱みについて言及を行うことである。
- 対象とする技術は、機器の脆弱性を突いたり、内部ノードをマルウェア感染させること等により、ネットワークを経由してローカルシステムへ侵入し、不正な動作が行われたことを検知、検出するための技術であり、脅威インテリジェンス、侵入／異常検知、ウイルス／マルウェア検知、それらの適用領域に着目する。また、検知におけるAIの利用やAIに対する攻撃対策についても着目する。
- 調査の対象とする文献は、特許文献と論文である。特許文献は2017～2023年(優先権主張年ベース)の日本、米国、欧州、中国、韓国、イスラエル、インド、ロシアへの出願及び登録特許とPCT出願で、論文は2017～2024(発行年ベース)を対象とし、目視によるノイズ除去を行った上で解析を実施している。ノイズ除去を行った結果、特許文献については21,241件のパテントファミリーを対象に、論文は16,389件を対象に、解析を実施した。

なお、特許文献の調査結果を第４章に、論文の調査結果を第５章に取りまとめている。

要約

第１節　調査の目的

特許情報から技術全体を俯瞰し、経済情報・産業情報を踏まえた技術開発の進展状況・方向性を把握することは、特許庁における審査体制の構築や的確かつ効率的な審査等のための基礎資料の整備、さらには産業政策、科学技術政策の基礎資料の整備をする上で必要である。

また、今後、我が国の産業が持続的に発展していくためには、新規事業の創出が不可欠であり、そのためには、企業や大学・公的研究機関等の技術開発、知財戦略策定を支援していく必要がある。特許情報はこれら企業等の研究開発動向、知財戦略の表れであり、技術開発、知財戦略の方向性を決定していく上でも重要なものである。

本報告書が対象とするサイバー攻撃検知技術(不正侵入・マルウェア等の検知に向けた情報セキュリティ技術)は、攻撃の早期把握や被害の拡大防止の観点から重要性が高まっている。特に、ランサムウェアは組織を標的とする脅威として注目が続いており(情報処理推進機構が毎年公表している情報セキュリティ 10 大脅威において直近 4 年で連続して組織における脅威の 1 位[1])、関連する技術情報も増えている。各国では法制度やガイドライン等の整備が進んでおり、制度面の動きも踏まえる必要がある。

なお、平成 27 年度に特許出願技術動向調査として情報セキュリティ技術全般に関する調査を実施しているが、その後、侵入検知・マルウェア検知の適用分野や技術動向は大きく変化している。したがって、侵入検知及びマルウェア検知に対象を限定し、最新の特許情報等を中心に動向を整理・分析することには意義がある。

加えて、当該分野の技術文献数の著しい増加に伴い、文献調査の困難度が高まっているところ、最新の技術動向・出願動向を把握することは今後の特許審査においても有益であると考えられる。

このような背景のもと、「サイバー攻撃検知技術～不正侵入・マルウェア等の検知に向けた情報セキュリティ技術～」に関する技術革新の状況、技術競争力の状況、今後の展望等について検討する必要がある。

本調査報告書では、サイバー攻撃検知技術(不正侵入・マルウェア等の検知に向けた情報セキュリティ技術)に係る技術に関する市場動向、政策動向、特許動向、研究開発動向等の最新の動向について、調査・分析結果を記す。そして、本調査の分析結果に基づき、本テーマにおける国内外の技術発展状況、研究開発状況を含む技術動向、日本及び外国の技術競争力、産業競争力を明らかにするとともに、日本企業・政府機関が取り組むべき課題を整理し、今後目指すべき研究・技術開発の方向性を明らかにすることを目的とする。

第２節　調査対象範囲

１．　技術俯瞰図

本調査はサイバー攻撃検知技術(不正侵入・マルウェア等の検知に向けた情報セキュリティ技術)に係る技術を調査対象としており、具体的には、機器の脆弱性(セキュリティ

[1] 情報処理推進機構(情報セキュリティ 10 大脅威 2025[組織])(2025 年 1 月 30 日公開)
(https://www.ipa.go.jp/security/10threats/10threats2025.html)

ホール)を突くこと、あるいは、機器の内部構成に対してマルウェア感染させること等により、ネットワークを経由してローカルシステムへ侵入し、不正な動作が行われたことを検知、検出する技術であり、例えば、ローカルシステム内で不正な命令を実行させる、ローカルシステム内の機密情報へアクセスする等がこれに含まれる。ここでローカルシステムには、組織内ネットワークシステムに限定せず、コンピュータ、スマートフォン等の計算機単体や車載ネットワークシステム等も含まれる。また、不正に認証を突破し、個人のアカウントにログインするものは、本調査の対象に含めていない。

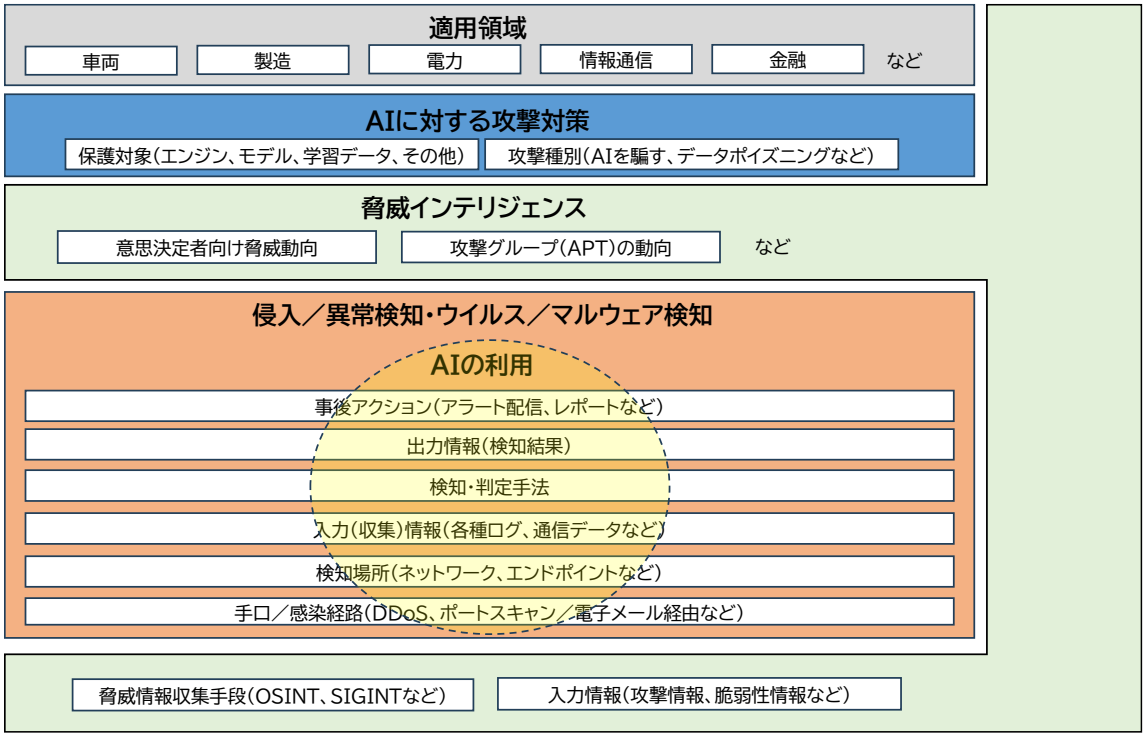
図 1-2-1 に、本調査が対象とする技術領域を表す技術俯瞰図を示す。この図は、侵入／異常検知・ウイルス／マルウェア検知と、これに関連する脅威インテリジェンス、AI に対する攻撃対策、及び対象技術が適用される産業領域の関係性を示す概念図である。「①情報の収集」「②検知・判定」「③分析」「④応用・適用先」という概念的な処理の流れを下から上に時系列で示している。

図の下から順に、入力側の脅威インテリジェンス(薄緑色部分)、侵入／異常検知・ウイルス／マルウェア検知(中央オレンジ色部分)、出力側の脅威インテリジェンス(薄緑色部分)、AI に対する攻撃対策(濃青色部分)を配置し、その上に適用領域(灰色部分)を配置した。また、侵入／異常検知・ウイルス／マルウェア検知(中央オレンジ色部分)においても、下から上に向かって時間軸が順方向となるよう手口／感染経路、検知場所、入力情報、検知・判定手法、出力情報、事後アクションを配置した。加えて、AI 技術の進展に伴い、各技術項目で AI が利用されるようになっていることから、AI 技術が含まれるものを点線で示した。さらに、その上に対象技術の応用先として AI に対する攻撃対策、及び対象技術が適用される産業領域を配置した。

なお、上述の処理の流れは、情報処理推進機構(IPA)による「脅威インテリジェンス導入・運用ガイドライン」[2]に示される「サイバーセキュリティに関する脅威情報を収集・加工し、また、それらを分析することによって得られるインテリジェンスに基づく組織のセキュリティ対応における意思決定のライフサイクル」に対応するものである。このライフサイクルは、「方針策定」「収集・加工」「分析」「配布」「評価」の 5 つのフェーズから構成される。この中で「収集・加工」フェーズでは、セキュリティニュース等の OSINT(Open-Source Intelligence)、セキュリティ機器から収集したログ等の SIGINT(Signal Intelligence)、それらを加工した脅威アクター(個人・組織・グループ等の脅威主体)等、脅威情報が収集される。脅威情報はサイバー攻撃検知の入力情報として利用される。また、「収集・加工」フェーズで得られた情報を組織のセキュリティ対策の意思決定に必要なインテリジェンスへと昇華するフェーズである「分析」フェーズにおいては、自組織でのサイバー攻撃検知結果も利用される。

[2] 情報処理推進機構(脅威インテリジェンス導入・運用ガイドライン「2.1.1 脅威インテリジェンスの定義」)(2024 年 7 月発行)
(https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003510-att/f55m8k000000358r.pdf)

図 1-2-1　技術俯瞰図



2．　対象技術の概要

（1）　脅威インテリジェンス

「脅威インテリジェンス」の定義は取り扱われる組織や媒体によって異なり、例えば、第 1 節で示したようにライフサイクルそのものを「脅威インテリジェンス」と呼ぶ場合もある。本調査では、「サイバー攻撃検知技術」との関連を分かりやすくするため、下記①、②の要素を含む総称を「脅威インテリジェンス」と呼ぶ。

①　「脅威インテリジェンス(狭義)」

サイバーセキュリティに関する脅威情報を収集・加工し、また、それらを分析することによって得られるインテリジェンスに基づく情報で、組織のセキュリティ対応における意思決定者向けの脅威動向や攻撃グループの動向を含む。

②　「脅威情報」

「脅威インテリジェンス(狭義)」のライフサイクルにおいて、第 2 部の市場動向調査で取り上げるツール等により収集される情報(IP アドレス、マルウェアハッシュ、ツール名等)と当該ツールにより前記情報が加工された後に出力される情報(脅威アクターの識別情報、侵入・感染経路等の情報)。

前者の「脅威インテリジェンス(狭義)」は後述する侵入／異常検知・ウイルス／マルウェア検知の結果を分析して出力される情報であり、後者の「脅威情報」は侵入／異常検知・ウイルス／マルウェア検知の入力情報である。

（2）　侵入／異常検知・ウイルス／マルウェア検知

本調査では、侵入／異常検知・ウイルス／マルウェア検知の処理の流れに沿って、検

知対象を表す手口・感染経路、どこで検知を行うかを表す検知場所、検知に利用する入力情報、検知・判定に利用される手法、検知結果としての出力情報、検知後の事後アクションを調査対象とした。それぞれの概要を以下に示す。

① 手口

不正アクセスや不正侵入等のサイバー攻撃の手段。DoS/DDoS 攻撃、ポートスキャン、システムやソフトウェアの脆弱性を利用した侵入、電子メール・Web サイト経由・その他のアプリケーション経由の侵入、ボットネット、踏み台、フィッシング、ランサム攻撃、ゼロデイ攻撃、サプライチェーン攻撃、サイドチャネル攻撃、AI を利用したサイバー攻撃等を含む。サイバー攻撃の検知に用いる悪性 URL 等の脅威インテリジェンス(脅威情報)を収集する技術も含む。ただし、悪性プログラム(ウイルス／マルウェア等)に関するものは除く。

② 感染経路

悪性プログラム(ウイルス／マルウェア等)の感染経路。電子メール配布、Web サイト配布、その他のアプリケーション配布、脆弱性からの感染、ボットネット、踏み台、ゼロデイ攻撃、サプライチェーン攻撃、AI を利用した感染等を含む。

③ 検知場所

サイバー攻撃やウイルス／マルウェアの検知を行う監視場所。検知を行う組織が管理しているネットワーク(内部ネットワーク)、内部ネットワークとインターネット等の検知を行う組織が管理していないネットワークとの間(境界)、PC やサーバ等のエンドポイント等を含む。エンドポイントの監視とネットワークの監視を統合してより高度な監視を行う場合(広域・総合的)も含む。

④ 入力情報

サイバー攻撃や悪性プログラム(ウイルス／マルウェア等)の検知に利用する情報。セキュリティ運用ログ、トラフィックログ、アプリケーションログ、システムログ、その他保存データ、通信データ、脅威情報・脆弱性情報等を含む。AI の普及を考慮して、AI を利用した入力(収集)情報も調査対象とした。

⑤ 検知・判定手法

不正アクセスや不正侵入、あるいは悪性プログラム(ウイルス／マルウェア等)等のサイバー攻撃の検知・判定をするための手法。パターンマッチング手法、静的ヒューリスティック手法、動的ヒューリスティック手法、ログ解析、チェックサム方式、相関分析等の複数のデータを統合した解析、コネクトバック通信の検知、Sandbox、AI を利用したログ解析等を含む。

⑥ 出力情報

サイバー攻撃や悪性プログラム(ウイルス／マルウェア等)の検知結果の出力としての情報。2 値(0／1)、3 段階以上のレベル又はスコア、侵入経路、攻撃元情報、リスク判定結果等を含む。

⑦ 事後アクション

サイバー攻撃や悪性プログラム(ウイルス／マルウェア等)への感染を検知した後の対処。アラート配信・レポーティング、回復アクション、AI を利用した事後アクション等を含む。

（3） AIに対する攻撃対策

AIに対する攻撃としては、例えば、GAN(敵対的生成ネットワーク)を利用して、AIを騙すノイズを付加した画像(敵対的サンプル画像)を生成し、画像による識別を妨害する攻撃や、プロンプトを工夫して倫理的な制約等で本来AIが意図しない結果を出力させる攻撃等AIを騙す攻撃、訓練データを汚染させることにより学習モデルによる誤分類やパフォーマンス低下を招くデータポイズニング攻撃、モデル抽出攻撃やメンバーシップ推論攻撃、モデルインバージョン攻撃等AIから学習データやモデルを詐取・推知する攻撃等が存在する。サイバー攻撃検知技術はこれらのAIに対する攻撃対策としても適用される。

（4） 適用領域

サイバー攻撃検知技術は、種々の産業分野に適用されるが、本調査では、主な適用分野を識別する区分として、車両、製造、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、港湾、交通システム、教育、学術研究を設定した。

第3節 技術区分表

特許文献及び論文を詳細に読み込み、技術区分を付与する際に用いた技術区分表と付与ルールを表1-3-1～表1-3-8に示す。技術区分は大区分、中区分、小区分の多階層とした。技術俯瞰図で示した「侵入／異常検知」「ウイルス／マルウェア検知」「脅威インテリジェンス」「AIに対する攻撃対策」「適用領域」の5つに加えて、さらに、「侵入／異常検知」と「ウイルス／マルウェア検知」で共通の項目である「検知共通」「解決課題／効果」、及び「侵入／異常検知」と「ウイルス／マルウェア検知」以外の検知に関する「その他(検知)」の3つを含めた、合計8つの大区分を設けた。なお、付与ルールに特段に記載のない場合は、特許文献の場合は発明の名称・要約・請求項・課題・解決手段・実施例を対象に、論文の場合は抄録を対象に分析する。

表 1-3-1　技術区分表と付与ルール(侵入／異常検知)

大区分	中区分	小区分	記号	説明	付与ルール
A 侵入／異常検知			A		
	a手口		Aa		
		01 DoS/DDoS攻撃	Aa01	サーバに大量のリクエストを送ることでサービスを機能停止させる攻撃(DoS攻撃：Denial of Service attack)。複数のコンピュータを利用して一斉に攻撃を仕掛ける場合は、DDoS攻撃(Distributed Denial of Service attack)と呼ぶ。	
		02 ポートスキャン	Aa02	ネットワークに接続された機器のTCPやUDPの様々なポート番号に接続を試み、応答を調べること。攻撃者が標的のシステムを調べ、攻撃に使えそうな脆弱性のあるポートがないか探すために行われる。	
		03 脆弱性からの侵入	Aa03	ソフトウェア製品、PCクライアントソフトウェア、Webアプリケーションの脆弱性を悪用して攻撃・侵入する。	エクスプロイト(OSやソフトウェア等の脆弱性を突いた攻撃や、脆弱性を狙うプログラム)を用いるものを含む。バックドアからの侵入を含む。 管理体制や業務手順等ヒトに起因する脆弱性は対象外。 他の小区分と組み合わせて付与してよい。
		04 電子メール経由	Aa04	電子メールを経由して侵入・攻撃を行う。	マルウェア感染、スパイウェアインストール、認証情報の取得、デマの拡散等の目的でメールを送りつける。スパムメール、標的型メール、フィッシングメールを含む。
		05 Webサイト経由	Aa05	Webサイトを経由して侵入・攻撃を行う。	SNS経由を含む。
		06 その他のアプリケーション経由	Aa06	電子メール／Webサイト以外のアプリケーションを経由して侵入・攻撃を行う。	電子メール／Webサイト以外のあらゆるアプリケーションが対象。
		07 ボットネット、踏み台	Aa07	ゾンビPC(サイバー攻撃により乗っ取られたPC)、管理者権限を第三者に不正に取得された、あるいは、マルウェア等に感染したサーバや端末。	
		08 フィッシング	Aa08	信頼できるソースからのメールやWebサイトに見せかけて、悪性のWebサイトに誘導したり、個人情報を入力させたりする攻撃。	フィッシングメール、フィッシングサイトを含む。 他の小区分と組み合わせて付与してよい。
		09 ランサム攻撃	Aa09	攻撃者がターゲットとなるシステムやネットワークに侵入し、身代金の支払いと引き換えに組織または個人を脅迫するために用いる方法。重要なデータを暗号化する、端末をロックして使用できなくする動作や機密情報を公表するとの脅し等を行い、身代金を要求する。	他の小区分と組み合わせて付与してよい。
		10 ゼロデイ攻撃	Aa10	ソフトウェア等にセキュリティ上の脆弱性が発見された時に、問題の対処や対策法(パッチ配布等)が広く周知される前に行われる攻撃。	他の小区分と組み合わせて付与してよい。
		11 サプライチェーン攻撃	Aa11	関連企業や取引先企業等を経由して攻撃をしかけるタイプのサイバー攻撃。標的となる大企業と取引関係のある中小企業や子会社を経由して侵入する「ビジネスサプライチェーン攻撃」、クラウドサービス事業者やITインフラ管理会社(MSP)等、企業が利用している外部サービス提供者を攻撃し、間接的に標的企業へ侵入する「サービスサプライチェーン攻撃」。	サプライヤーのネットワークを経由した侵入、大手メーカーの主要部品部品サプライヤーがランサムウェア等の攻撃を受けた結果、大手メーカーの部品調達システムに影響が及ぶケース、委託先PCに侵入され、クラウド上の顧客情報流出を招くケース等が含まれる。 他の小区分と組み合わせて付与してよい。
		12 サイドチャネル攻撃	Aa12	装置の物理的な特性の変化を外部から観測・解析することにより、意図しない経路から情報を漏洩させる攻撃。タイミング攻撃、差分電力攻撃等を含む。	サブリミナル(カバート)チャネル。 G06F21/55,360(カバートチャネル、即ち、プロセス間のデータ漏洩の防止を含むもの)及び380(差分電力攻撃への対抗手段を備えるもの)に対応。
		13 AIを利用した攻撃	Aa13	攻撃自体にAIを利用するもの。	攻撃シナリオをAIに検討させるものを含む。他の小区分と組み合わせて付与してよい。
		14 その他の手口	Aa14	USBやOBD(On-Board Diagnostics)等の外部メディアを介した攻撃等。その他の手口で攻撃・侵入する。	USB経由、車載式故障診断装置OBD(On-Board Diagnostics)経由、内部不正を含む
	b検知・判定手法		Ab		
		01 パターンマッチング手法	Ab01	ネットワークのパケットやアクセスログの特徴的な部分をパターンとしてデータベース化し、検索対象のパケットまたはアクセスログの内容と照合(マッチング)させる方法。シグネチャ検知、攻撃のパターンを定義したブラックリスト／ホワイトリストファイルを用いる手法も含む。閾値をもとに侵入や異常を判定する方法も含む。	照合されるパターンが動的なものを含む。
		02 ログ解析	Ab02	システムログ等の各種ログから攻撃と思われる痕跡を検出し判定する。通信データ等によるデータ解析も含む。	
		03 チェックサム方式	Ab03	ファイルや通信データのハッシュ値、チェックサム、フィンガープリント等を計算して既知のデータと比較することでデータが改ざんされていないかを確認する。	
		04 統合解析	Ab04	相関分析、自己相関分析、ベイズ推定等に基づいてインシデント危険度や攻撃パターンの変化、通常とは異なる挙動等を検出する。	収集したログに基づいて、複数の情報源から取得した情報の相関関係の分析結果を検知に利用するもの。
		05 AIを利用した検知・判定手法	Ab05	検知・判定にAIを利用するもの。	他の小区分と組み合わせて付与してよい。
		06 その他検知・判定手法	Ab06	上記以外の検知・判定手法を対象とする。	
	cその他侵入／異常検知		Ac		
		01 その他侵入／異常検知	Ac01	その他の侵入検知に関する事項に付与する。	

要約

表 1-3-2　技術区分表と付与ルール(ウイルス／マルウェア検知)

大区分	中区分	小区分	記号	説明	付与ルール
B ウイルス／マルウェア検知			B		
	a感染経路		Ba		
		01 電子メール配布	Ba01	電子メールに添付されているファイルを開くことで感染。	ウイルス／マルウェアに感染させる目的のもの。悪意ある第三者からのメールだけでなく、知らずに転送されたメールも含む。他の小区分と組み合わせて付与してよい。
		02 Webサイト配布	Ba02	不正サイトからの配布。(管理者に気づかれずに)改ざんされたサイトからの配布。	正規管理者以外が制御するサイトを含む。マルウェアに感染させる目的のもの。ドライブバイダウンロード攻撃はこちらに付与。C2サーバからのダウンロードも含む。
		03 その他のアプリケーション配布	Ba03	不正コードを含むアプリケーションの配布で、電子メール／Webサイト配布に該当しないもの。	ネットワークを介してダウンロードされるソフトウェアやアプリケーションを介して感染する攻撃、ソフトウェアの更新を悪用した攻撃、ファイル共有ソフトから入手したファイルからの感染等を含む。
		04 脆弱性からの感染	Ba04	ソフトウェア製品、PCクライアントソフトウェア、Webアプリケーションの欠陥等、脆弱性を介して感染する。	バックドアを利用した感染も含む。 他の小区分と組み合わせて付与してよい。
		05 ボットネット、踏み台	Ba05	マルウェアをばらまくために悪意のない第三者の資源を利用するもの。ゾンビPC、サーバ、ルータ等。	マルウェアに感染させる目的のもの。感染した結果として感染を広げる機能を持つものを含む。
		06 ゼロデイ攻撃	Ba06	パッチ公開前の脆弱性に対する攻撃、未知のウイルス／マルウェアを含む。	パッチが公開されていない亜種マルウェアも含む。
		07 サプライチェーン攻撃	Ba07	関連企業や取引先企業等を経由して攻撃をしかけるタイプのサイバー攻撃。ソフトウェア製品の製造工程や流通工程においてプログラムに混入させた不正コードの実行によりユーザや企業に損害を与える「ソフトウェアサプライチェーン攻撃」、標的となる大企業と取引関係のある中小企業や子会社を経由して侵入する「ビジネスサプライチェーン攻撃」、クラウドサービス事業者やITインフラ管理会社(MSP)等、企業が利用している外部サービス提供者を攻撃し、間接的に標的企業へ侵入する「サービスサプライチェーン攻撃」。	ソフトウェアの開発プロセスへの介入、流通過程でのプロダクト改ざん、サプライヤーのネットワークを経由したマルウェア感染、大手メーカーの主要部品部品サプライヤーの端末等がマルウェアに感染した結果、大手メーカーの部品調達システムに影響が及ぶケース、委託先PCのマルウェア感染からクラウド経由で情報流出を招くケース等が含まれる。 他の小区分と組み合わせて付与してよい。
		08 AIを利用した感染	Ba08	感染自体にAIを利用するもの。	感染させるためのシナリオをAIに検討させるものを含む。他の小区分と組み合わせて付与してよい。
		09 その他の感染経路	Ba09	USB等の外部メディアを介した感染等、その他の感染経路。	内部不正を含む。
	b検知・判定手法		Bb		
		01 パターンマッチング手法	Bb01	既知の不正コードとの類似性に基づくマルウェア検知。シグネチャベースのマルウェア検知、攻撃のパターンを定義したブラックリスト／ホワイトリストファイルを用いる手法も含む。閾値をもとにウイルス／マルウェアを検知したかどうかを判定する方法も含む。	照合されるパターンが動的なものを含む。
		02 静的ヒューリスティック手法	Bb02	コードを実行せずに分析し、悪性プログラム(ウイルス／マルウェア等)かどうかを判断する方法。	
		03 動的ヒューリスティック手法	Bb03	プログラムを実際に動かして、その挙動を見て悪意があるかどうか判断する方法。	
		04 統合解析手法	Bb04	相関分析、自己相関分析、ベイズ推定等に基づいて通常とは異なる挙動等を検出する。	収集したログに基づいて、複数の情報源から取得した情報の相関関係の分析結果を検知に利用するもの。
		05 コネクトバック通信の検知	Bb05	C2サーバ(Command and Control server)との通信を検知する。攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェアが仕掛けられたコンピュータの動作を制御するために用いられる通信の検知に関する事項を含む。	C2サーバは、攻撃者がマルウェアに感染したコンピュータを遠隔で操作・制御(Command & Control)するために利用するサーバ。
		06 チェックサム方式	Bb06	検査ファイルにあらかじめ付加されたチェックサム値(感染前のファイルの容量やハッシュ値等)と、検査ファイルから何らかの方法で計算されるチェックサム値を照合する手法。	
		07 Sandbox	Bb07	疑わしいプログラムを隔離された領域(Sandbox)で実行することにより、他に悪影響を及ぼさないように分析等する仕組み。	上記の手法をSandbox上で実施する点に特徴がある場合は、重複して付与。「Sandboxで実施しても良い」等特徴がない場合は付与しない。
		08 AIを利用した検知・判定手法	Bb08	検知・判定にAIを利用するもの。	他の小区分と組み合わせて付与してよい。
		09 その他の検知・判定手法	Bb09	上記以外の検知・判定手法。	
	cその他ウイルス／マルウェア		Bc		
		01 その他ウイルス／マルウェア	Bc01	その他のウイルス／マルウェア検知に関する事項に付与する。	

表 1-3-3　技術区分表と付与ルール(検知共通)

大区分	中区分	小区分	記号	説明	付与ルール
C 検知共通			C		
	a検知場所		Ca		
		01 組織外部のネットワーク	Ca01	組織から見て外部のネットワークを監視するもの。通信事業者、クラウドサービス等の事業者が管理するネットワークの監視。	当該サービス提供者が主体となって行うもの。 EDR(Endpoint Detection and Response)、 NDR(Network Detection and Response)、 XDR(eXtended Detection and Response)を用いてもよい。
		02 ネットワーク境界部	Ca02	企業等組織の内部ネットワークとインターネットとの間に設置する機器を用いて不正なアクセスや攻撃を検知するもの。	典型的には、FW(FireWall)、IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)等を用いる場合が含まれる。
		03 内部ネットワーク	Ca03	組織内のネットワークを監視。	典型的には、NDR(Network Detection and Response)を用いる場合が含まれる。
		04 エンドポイント	Ca04	エンドポイントを監視して攻撃及びその兆候を検出するもの。監視対象にサーバ、PC、モバイルデバイス、IoT製品、ECU(Electronic Control Unit)等を含む。	典型的には、EDR(Endpoint Detection and Response)、EPP(Endpoint Protection Platform)、ウイルス対策ソフトウェア、エージェント等を用いる。 ECUは、車両制御用のコンピュータ。
		05 広域・総合的	Ca05	エンドポイントの監視とネットワークの監視を統合してより高度な監視を行うもの、攻撃の検出に加えて、攻撃の兆候の検出も含む。	XDR(eXtended Detection and Response)と言及されていなくても、明細書及び図面から判断する。課題や効果についての記載が参考になる場合がある。
		06 その他検知場所	Ca06	上記のいずれにも該当しないもの。	検知場所が特定される場合はその検知場所を備考欄(文献に紐づけて別途設ける)に記載。
		07 検知場所に関する記載がない	Ca07	監視・検知を行っているが、場所の記載がないもの。	サイバーセキュリティと無関係の文献(ノイズ)は別の備考欄に記入。
		08 記載が不明確で読み取れない	Ca08	監視・検知場所に関する記載があるが、不明確で上記のどこに該当するか判断できない。	
	b入力(収集)情報		Cb		
		01 セキュリティ運用ログ	Cb01	セキュリティイベントを監視するログであって、特定のリソースへのアクセスログや機密ファイルへのアクセスの記録、ログオン・ログアウト等を含む。	【侵入/異常検知】侵入／異常検知処理の際に参照するものに付与。 【マルウェア検知】ウイルス／マルウェア検知処理の際に参照するものに付与。 リスク評価のためのログ分析が主目的なら対象外。
		02 トラフィックログ	Cb02	ファイアウォールを通過したトラフィックを記録する、特定のユーザによるアクセス状況を記録する等。	同上
		03 アプリケーションログ	Cb03	アプリケーションまたはプログラムによって発生したイベントを記録したデータを対象とする。	同上
		04 システムログ	Cb04	システムの活動によって生成されるログ。カーネルログ、OSログ、サーバログ等を含む。 ・システムを構成するリソースの物理的状況 ・ハードウェアの認識の有効・無効状態 ・システム動作状態 ・リソース状況 ・サービスへのアクセス記録 ・エラー状況	同上
		05 その他保存データ	Cb05	上記以外の保存データ(DBデータ、設定ファイル、検知対象以外のプログラム等)。	同上
		06 通信データ	Cb06	通信の時系列データそのもの。ログ収集目的ではなく、リアルタイムに検知に利用されるもの。	検知対象のパケット、信号、イベント等。データの態様を限定しない。
		07 脅威情報・脆弱性情報等	Cb07	外部サービス等を利用して入手する脅威情報と、システム内分析結果を利用する場合も含む。公開されている脆弱性情報。意図せず公開されている機器情報や設定情報等を含む。	【侵入／異常検知】攻撃パターンを定義したデータベース等の更新、侵入／異常検知処理の際に利用するものに付与。 【マルウェア検知】ウイルス定義ファイル等の更新、ウイルス／マルウェア検知処理の際に利用するものに付与。
		08 AIを利用した入力(収集)情報	Cb08	入力(収集)情報にAIを利用する。	
		09 その他の入力(収集)情報	Cb09	その他の情報。	
	c出力情報(検知結果)		Cc		
		01 0／1	Cc01	侵入あり／なし、陽性／陰性。	
		02 3段階以上のレベル又はスコア	Cc02	確度、判定結果の信頼度等を算出するもの。	偽陽性を区別するものは、こちらに付与。
		03 侵入経路	Cc03	検知した段階で経路を特定するもの。	
		04 攻撃元情報	Cc04	攻撃の起点を特定できる場合。	IPアドレスの特定に限定せず、ドメインや国の特定でもよい。
		05 リスク判定結果	Cc05	攻撃検知と合わせてリスク算出、リスク判定を行う場合。	リスクあり／なしだけでなく、リスクの度合を数値等で出力する場合も含む。
		06 その他	Cc06	付加的な出力がある場合。	
	d事後アクション		Cd		
		01 アラート配信	Cd01	サイバー攻撃(不正侵入、ウイルスやマルウェア等)が検知された際にアラームや通知を行う場合を対象とする。アラート形式(メール、電話、アラーム等)は限定しない。侵入あり／なし、陽性／陰性等の検知結果を出力する記載がある場合を含む。ただし、レポーティング(レポートの通知、分析結果の通知等)を行う場合は除く。	
		02 レポーティング	Cd02	サイバー攻撃(不正侵入、ウイルスやマルウェア等)が検知された際にレポーティング(レポートの通知、分析結果の通知等)を行う。レポートの形式(メール、電話、報告書等)は限定しない。	
		03 回復アクション	Cd03	アクセス制御、分離・遮断、事後対応の準備、不正アクセスの追跡等を含む。ウイルスやマルウェアが検知された際に回復アクションを行う。マルウェアの無毒化／無害化を含む。	ウイルス対策ソフト、EPP(Endpoint Protection Platform)等を用いたウイルス除去や分離・遮断等を含む。
		04 AIを利用した事後アクション	Cd04	事後アクション(攻撃手段やマルウェアの分析、不正アクセスの追跡等)にAIを利用する。	
		05 その他	Cd05	その他の事後アクション。	

表 1-3-4　技術区分表と付与ルール(その他(検知))

大区分	中区分	小区分	記号	説明	付与ルール
D その他(検知)			D		
	aその他AIを利用		Da		
		01 その他AIを利用	Da01	その他の侵入／異常検知、ウイルス／マルウェア検知にAIを利用する。	
	bその他(検知)		Db		
		01 その他(検知)	Db01	その他の侵入／異常検知、ウイルス／マルウェア検知に関する事項に付与する。	

表 1-3-5　技術区分表と付与ルール(適用領域)

大区分	中区分	小区分	記号	説明	付与ルール
E 適用領域(産業等)			E		
	a重要インフラ		Ea		
		01 重要インフラ	Ea01	サイバーセキュリティ基本法第12条第2項第3号に定める重要インフラにおいて、重要インフラサービスの継続的提供を不確かなものとするサイバー攻撃に関わるもの。	特定の分野が明示的に記載されている場合に付与。情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、港湾：該当するものを備考欄に記入。
	bその他特定業種・セクター		Eb		
		01 その他特定業種・セクター	Eb01	上記以外の産業分野で特定の業種に適用される旨言及されているもの。	特定の分野が明示的に記載されている場合に付与。例)製造、車両、交通システム、教育、学術研究；該当するものを備考欄に記入。
	c汎用		Ec		
		01 汎用	Ec01	多種多様な業種・業態に適用可能と言及されているもの。	明示的に複数の分野が記載されている場合に付与。重要インフラとそれ以外を多数含むもの。
	d記載なし		Ed		
		01 記載なし	Ed01	産業上の適用領域について記載のないもの。	

表 1-3-6　技術区分表と付与ルール(解決課題／効果)

大区分	中区分	小区分	記号	説明	付与ルール
F 解決課題／効果			F		
	a機能性向上		Fa		
		01 検知精度の向上	Fa01	誤検知／過検知、検知漏れの低減。	目的、課題、効果として言及しているもの。
		02 適用範囲の拡大	Fa02	監視対象の拡大。	同上
		03 検知の高度化	Fa03	複合的な手法によるもの、複雑な事象(巧妙な攻撃手法やマルウェア感染手法)の検知。	同上
	b効率化		Fb		
		01 人による判断のシステム化・自動化	Fb01	セキュリティ専門家が行う高度な判断の自動化による効率化。	目的、課題、効果として言及しているもの。
		02 手動作業のシステム化・自動化	Fb02	手動作業の自動化による効率化。	同上
		03 処理の高速化	Fb03	検知・事後アクション等の処理の高速化による効率化。	目的、課題、効果として言及しているもの。(パッチを当てるまでの時間短縮は、今回の対象外)
	cその他(不明含む)		Fc		
		01 その他(不明含む)	Fc01	上記以外の課題や効果。またはそれらが不明のもの。	

表 1-3-7　技術区分表と付与ルール(AI に対する攻撃対策)

大区分	中区分	小区分	記号	説明	付与ルール
G AIに対する攻撃対策			G		
	a保護対象		Ga		
		01 エンジン	Ga01	AIエンジン(AIの核となるプログラム等の集合。AIシステム)を保護する。	
		02 モデル	Ga02	AIモデルを保護する。	
		03 学習データ	Ga03	学習データを保護する。	
		04 その他の保護対象	Ga04	上記以外のAI関連要素を保護する。	
	b攻撃種別		Gb		
		01 AIを騙す攻撃	Gb01	GAN(敵対的生成ネットワーク)を利用して、AIを騙すノイズを付加した画像(敵対的サンプル画像)を生成し、画像による識別を妨害するもの。倫理的な制約等で本来AIが意図しない出力をプロンプトを工夫して出力させるもの等。これらの攻撃に対抗する技術に付与。回避攻撃とも呼ばれる。	識別情報は、顔画像に限定されず、車両のナンバープレート等も対象。
		02 データ・ポイズニング攻撃	Gb02	訓練データを汚染させることにより学習モデルによる誤分類やパフォーマンス低下を招く攻撃。この攻撃に対抗する技術に付与。	
		03 データ等の詐取・推知	Gb03	モデル抽出攻撃、メンバーシップ推論攻撃、モデルインバージョン攻撃等のAIから学習データやモデルが詐取・推知されるもの。この攻撃に対抗する技術に付与。	
		04 その他の攻撃手法	Gb04	上記以外のAIに対する攻撃に対抗する技術に付与。	

表 1-3-8　技術区分表と付与ルール(脅威インテリジェンス)

大区分	中区分	小区分	記号	説明	付与ルール
H 脅威インテリジェンス			H		
	a脅威情報収集手段		Ha		
		01 Open Source INTelligence(OSINT)	Ha01	公開情報からデータ収集。	セキュリティに関するニュース、公的機関が公表する注意喚起情報、Webサイト、DNS等公開サーバから合法的に取得できる情報、個人、団体が公開している脅威情報。
		02 HUMan INTelligence(HUMINT)	Ha02	人を介してデータ収集。	組織内部通報、有償の脅威インテリジェンスベンダからの情報、業界コミュニティの情報共有、ダークウエブ、Telegram上のコミュニティやり取り。
		03 SIGnal INTelligence(SIGINT)	Ha03	機器やデバイス、システムのアラートやログ等のデータを収集。	Proxyログ、IDS/IPS、EDRのアラート、SIEMログ。
		04 デセプション	Ha04	悪意のある攻撃を受けやすいように設定した機器(ハニーポット)や欺瞞環境を、おとりとしてネットワーク上に公開することにより、サイバー攻撃を誘引し、攻撃者の特定や攻撃手法を分析する手法、あるいは、そのような用途で使用するシステム。	
	b入力情報(収集情報)		Hb		
		01 セキュリティニュース	Hb01	インシデント事例や脆弱性情報、セキュリティ動向等のニュースレポート。	
		02 攻撃手法	Hb02	攻撃者のTTPsに関するレポートやツール、フレームワーク等。	
		03 攻撃アクターの連携に関するチャットログの傍受	Hb03	攻撃者がターゲットとする組織に関する資産、脆弱性、攻撃手法。	
		04 マルウェア情報	Hb04	ウイルスを含むマルウェアを分析するためのサンプル自体や、マルウェア分析の結果(使用されたツールやファイル等のハッシュ値、挙動を含む)。	検体及びプログラムを含む。
		05 外部からのスキャンデータ	Hb05	外部から見える自組織の公開資産の状況。意図せず公開されている組込みシステム等のWebサイトにある機器情報や設定情報等。	外部(インターネット)から把握できる情報を用いてIT資産の適切な管理を可能とするツールやサービスを活用して、外部(インターネット)に公開されているサーバやネットワーク機器、IoT機器の情報を収集・分析することにより、不正侵入経路となりうるポイントを把握するASM(Attack Surface Management)。
	cその他脅威インテリジェンス		Hc		
		01 その他脅威インテリジェンス	Hc01	その他の脅威インテリジェンスに関する事項に付与。	

なお、本調査で対象とするセキュリティ製品及びサービスの定義を表 1-3-9 に示す。

表 1-3-9　調査対象のセキュリティ製品及びサービスの定義

セキュリティ製品及びサービス	定義
Endpoint Detection and Response (EDR)	エンドポイント（PC、サーバ、スマートフォン等）を常時監視し、異常な振る舞いをリアルタイムに検知し、遠隔から影響端末をネットワークから隔離したうえで、悪意あるプログラムの停止・削除などの対処を行う製品。
Network Detection and Response (NDR)	ネットワークトラフィックを継続的に監視・分析し、サイバー攻撃や不審な振る舞いを検知し、対処を行う製品。
Extended Detection and Response (XDR)	EDRの検知・対応範囲を拡張し、ネットワーク、クラウド、ID、メールなど複数のデータソースを統合して一元的に可視化・分析し、包括的な対処を行う製品。
Security Information and Event Management (SIEM)	ネットワーク機器、セキュリティ機器、データベース、クラウドサービス、クライアントPC等から出力されるセキュリティイベントログを収集・保管・分析・可視化する製品。
Security Orchestration, Automation and Response (SOAR)	複数の脅威情報やアラートを統合し、Orchestration（集約・分析・判断）、Automation（プレイブックに基づく自動処理）、Response（関係者への報告・通知）を通じてセキュリティ運用を自動化・効率化する製品及び機能。
脅威インテリジェンス提供サービス	セキュリティアナリストやホワイトハッカーが、インターネット、ダークウェブ、専門コミュニティなど多様な情報源から攻撃手法・攻撃者・標的等のデータを収集・解析し、組織に提供するサービス。
Managed Security Service (MSS)	セキュリティ機器・ログの監視やアラート通知など、組織のセキュリティに関わる運用を専門会社が代行するサービス。
Managed Detection and Response (MDR)	高度な検出技術と専門アナリストの知見を組み合わせ、脅威ハンティング、常時監視、インシデント対応をアウトソーシングサービスとして提供し、組織をサイバー脅威から保護するサービス。MSSより専門的で高度なサービス。
Firewall	外部からの不正アクセスや社内からの許可外通信を制御する機能や、拠点間・リモート接続用のVPN機能を有する製品。
Sandbox	未知のファイルやプログラムを本番環境とは分離した仮想環境で実行・観察し、ウイルスやマルウェア などの悪意ある挙動を検出する技術。

第４節　調査方法

１．　用語の説明

（１）　パテントファミリーの集計方法

①　パテントファミリー件数

いずれかの国・地域に出願された発明の数であり、同じ発明を複数の国・地域へ出願した場合にも１件と数える(1つの国・地域のみへ出願した場合も１件)。複数の国・地域へ出願した場合には、それらの出願のまとまりについて「パテントファミリー」又は「特許ファミリー」と称されることもある。

②　国際パテントファミリー(International Patent Family: IPF)件数

「国際パテントファミリー件数」とは、複数の国・地域への出願を含むパテントファミリーの件数、又は欧州特許庁(EPO)への出願若しくは PCT 出願(複数の国・地域での権利取得意志に基づくと推定される出願)を含むパテントファミリーの件数を意味する。

③　本調査で適用したパテントファミリー

本調査では Clarivate 社の Derwent Innovation で採用されるパテントファミリーを適用した。

（２）　欧州への特許出願と欧州籍の定義

本調査における欧州への出願とは、EPC(欧州特許条約)加盟国のうち DWPI に収録されているアイルランド、イタリア、オーストリア、オランダ、スイス、スウェーデン、スペイン、スロバキア、チェコ、デンマーク、ドイツ、トルコ、ノルウェー、ハンガリー、フィンランド、フランス、ベルギー、ポーランド、ポルトガル、ルーマニア、ルクセンブルク及び英国への出願並びに欧州特許庁への特許出願とする。

また、本調査における欧州籍の出願とは、出願人国籍・地域が EPC 加盟国であるアイスランド、アイルランド、アルバニア、イタリア、エストニア、オーストリア、オランダ、キプロス、ギリシャ、クロアチア、サンマリノ、スイス、スウェーデン、スペイン、スロバキア、スロベニア、セルビア、チェコ、デンマーク、ドイツ、トルコ、ノルウェー、ハンガリー、フィンランド、フランス、ブルガリア、ベルギー、ポーランド、ポルトガル、北マケドニア共和国、マルタ、モナコ、ラトビア、リトアニア、リヒテンシュタイン、ルーマニア、ルクセンブルク及び英国への特許出願とする。

（３）　2022 年以降の出願件数データに関する注意事項

検索を実施したのは 2025 年 8 月であり、2023 年の末から 18 か月が経過したばかりである。特許が出願されてから公開されるまでに 18 か月程度の期間を要すること、出願が公開されてからデータベースにデータが収録されるまでには発行国からデータベース会社にデータ提供されるまでの期間とデータベース会社の作業期間を要すること、また、PCT 出願の各国移行のずれがあること等のため、出願年が 2022 年あるいは 2023 年とする出願件数は全データを反映していない可能性がある。したがって、本調査報告書における 2022 年、2023 年の出願のデータは、真の値(今後の推移により定まる値)よ

り少ない可能性があることに留意されたい。

２．　特許詳細解析

（１）　調査の範囲

調査対象の特許文献

調査対象とした特許文献の種類は以下の通りである。

・PCT(特許協力条約)に基づく国際出願(以下、「PCT 出願」と呼ぶ。)
・日本、米国、欧州、中国、韓国、イスラエル、インド、ロシアへの特許出願
・日本、米国、欧州、中国、韓国、イスラエル、インド、ロシアでの登録特許
※調査対象の文献に実用新案は含まない。
※欧州については１．（２）　欧州への特許出願と欧州籍の定義を参照のこと。

時期的範囲

特許文献：2017-2023 年(優先権主張年ベース)

集計区分とする出願人国籍(地域)と出願人属性

出願件数の集計に当たっては、出願人の国籍(地域)として、日本、米国、欧州、中国、韓国、イスラエル、インド、ロシア、その他の区分に分計することとした。

出願人国籍、属性等の分析は筆頭出願人のデータを用いた。

（２）　調査の方法

使用データベース

特許文献の検索には、Clarivate 社が提供するデータベース Derwent Innovation-DWPI を使用した。

ファミリー単位での検索時にはファミリー単位での検索が可能な DWPI アクセッション番号を使用し、出力時には出願単位で出力を実施した。

特許検索式

特許分類とキーワードとを組み合わせた特許検索式により調査対象母集団を抽出した。特許検索式を表 1-4-1 に示す。

検索実施日は 2025 年 8 月 22 日である。

表 1-4-1　特許動向調査(詳細解析)の検索式

識別子	検索式	件数
クエリ 1	CC=(WO OR JP OR US OR EP OR CN OR KR OR IL OR IN OR RU)	
クエリ 2	PRD>=(20170101) AND PRD<=(20231231)	
クエリ 3	IC=(G06F002155 OR G06F002156)	
クエリ 4	IC=(H04L001200 OR H04W001200 OR H04L000900 OR H04L004300)	
クエリ 5	ALL=((attack or intrude or intrusion or unauthorised ADJ access or unauthorized ADJ access or unauthenticated ADJ access or infection or infect) NEAR5 (detect or detection or sensing))	
調査対象母集団の検索式	(クエリ 1 AND クエリ 2) AND (クエリ 3 OR (クエリ 4 AND クエリ 5))	52,973

表 1-4-1 に示すように、検索結果の出願数は 52,973 件であった。特許出願データの解析にあたっては、特許検索式で抽出された特許文献について、パテントファミリー単位で代表文献を選定した。代表文献の選定方法は、①パテントファミリーのうち日本語の一次文献(特許請求の範囲、明細書、図面、要約等。以下同じ)を代表文献とし、②前記パテントファミリーに日本語の一次文献が存在せず、英語の一次文献が存在する場合にあっては、当該英語の一次文献を代表文献とし、③前記パテントファミリーに日本語・英語の一次文献が存在せず、中国語又は韓国語のファミリー文献が存在する場合には、当該ファミリー文献を代表文献とし、④前記パテントファミリーに日本語・英語・中国語・韓国語の一次文献が存在しない場合にあっては、前記パテントファミリーのうちの一つの抄録、特許請求の範囲及び図面を解析対象とした。そのようにして、調査者が当該代表文献の読込み(詳細解析)を行い、技術区分表に規定された個々の技術区分への合致性を判定した。サイバー攻撃検知に関する記載がなく、本調査の対象外と判定されるものはノイズとして排除した。ノイズとして排除されなかった全パテントファミリー数は 21,241 件であった。

なお、特許検索式に現れる検索対象フィールドと演算子の意味は表 1-4-2 を、国際特許分類(IPC)の説明は表 1-4-3 を、それぞれ参照されたい。

表 1-4-2　特許検索式に現れる検索対象フィールド、演算子の説明

フィールド・演算子名	意味
CC	国コード
PRD	最先の優先主張日
IC	特許分類(IPC)
ALL	全文を対象に検索
ADJ	指定した順序で隣接する語句を含むレコードを検索
NEAR5	順不同で 5word 以内で隣接する語句を含むレコードを検索

表 1-4-3　国際特許分類(IPC)の説明

IPC	説明
G06	計算または計数
G06F	電気的デジタルデータ処理（特定の計算モデルに基づくコンピュータ・システムＧ０６Ｎ）
G06F21/00	不正行為から計算機，その部品，プログラムまたはデータを保護するためのセキュリティ装置［８，２０１３．０１］
G06F21/55	・・ローカルへの侵入を検知または対抗策を実行するもの［２０１３．０１］
G06F21/56	・・・コンピュータ・マルウェアの検出または処理，例．アンチ・ウィルス装置［２０１３．０１］
参考) G06F21/57	・・信頼された計算機プラットフォームの保証または維持，例．セキュアブートまたは電源断，バージョンの管理，システム・ソフトウェアの検査，セキュア更新または脆弱性評価［２０１３．０１］
H04	電気通信技術
H04L	デジタル情報の伝送，例．電信通信（電信通信と電話通信に共通の装置Ｈ０４Ｍ）［４］
H04L12/00	データ交換ネットワーク（メモリ，入力／出力装置または中央処理装置間の相互接続，またはそれらの間の情報または他の信号の転送Ｇ０６Ｆ１３／００）［５］
H04W	無線通信ネットワーク（放送通信Ｈ０４Ｈ；選択式通信によらない無線接続を用いる通信システム，例．ワイヤレスエクステンションＨ０４Ｍ１／７２）［２００９．０１］
H04W12/00	セキュリティ装置，認証，プライバシーまたは匿名の保護［２０２１．０１］

３．　拡大係数と特化係数

第４章では、縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布を調査している。本節ではそれぞれの定義を示す。

（１）　拡大係数

拡大係数(g_{ij})は、特定の技術区分が近年どの程度増加しているかを他国・地域との相対的指標として示す値であり、以下の式で定義される。

$$g_{ij} = \frac{Q_{ij}/q_{ij}}{\sum_j Q_{ij} / \sum_j q_{ij}}$$

Q_{ij} ：j国籍・地域による技術区分iにおける 2021-2024 年の合計出願件数

q_{ij} ：j国籍・地域による技術区分iにおける 2017-2020 年の合計出願件数

Q_{ij}/q_{ij} ：j国籍・地域による技術区分iにおける増加率

$\sum_j Q_{ij}$ ：技術区分i における2021-2024 年の全国籍・地域による累積件数

$\sum_j q_{ij}$ ：技術区分iにおける2017-2020年の全国籍・地域による累積件数
$\sum_j Q_{ij} / \sum_j q_{ij}$ ：技術区分iにおける全国籍・地域の平均増加率

拡大係数は、全国籍・地域の平均増加率で正規化しているため、拡大係数が1より大きければ「技術区分iにおける全国籍・地域の平均増加率」よりも大きく、拡大係数が1より小さければ「技術区分iにおける全国籍・地域の平均増加率」よりも小さい。そのため、ある技術区分における近年の出願件数の増加率を全国籍・地域平均に対する相対的な指標として評価したものであるといえる。

（2） 特化係数

特化係数(f_{ij})は、各国・地域における特定の技術区分の特許出願件数のシェアを他国・地域との相対的指標として示す値であり、以下の式で定義される。

$$f_{ij} = \frac{P_{ij} / \sum_i P_{ij}}{\sum_j P_{ij} / \sum_i \sum_j P_{ij}}$$

P_{ij} ：j国籍・地域における特定の技術区分iの出願件数
$\sum_i P_{ij}$ ：j国籍・地域における大区分内全技術区分の出願件数の合計
$P_{ij} / \sum_i P_{ij}$ ：特定の技術区分iの各国籍・地域jにおける構成比
$\sum_j P_{ij}$ ：全国籍・地域における特定の技術区分iの出願件数
$\sum_i \sum_j P_{ij}$ ：全国籍・地域における大区分内全技術区分の出願件数の合計
$\sum_j P_{ij} / \sum_i \sum_j P_{ij}$ ：全国籍・地域における技術区分iの構成比

特化係数は、ある技術区分のある国籍・地域における構成比を、ある技術区分の全国籍・地域の構成比で正規化していることから、特化係数が1より大きいか小さいかで、全国籍・地域平均の構成比に対して上位か下位かを示している。そのため、ある技術区分についての注力度を、全国籍・地域平均に対する相対的な指標として評価したものであるといえる。

4． 論文詳細解析

（1） 調査の範囲

調査対象の論文

調査対象とする論文は、検索データベースに収録されている論文を対象とし、英語及び英語にて検索できる論文とした。

時期的範囲

調査対象とする論文の時期的範囲は、発行年が2017年から2024年のものとした。

集計区分とする著者国籍(地域)

発表件数の集計に当たっては、著者の国籍(地域)として、日本、米国、欧州、中国、韓国、イスラエル、インド、ロシア、その他の区分に分計することとした。著者の分析は筆頭著者のデータを用いた。

（2） 調査の方法

使用データベース

論文の検索に使用したデータベースは、Clarivate 社が提供する Web of Science である。

論文検索式

キーワードを用いた検索式により調査対象母集団を抽出した。論文検索式を表 1-4-4 に示す。検索実施日は 2025 年 10 月 21 日である。

表 1-4-4 研究開発動向調査(詳細解析)の検索式

ステップ	クエリ	件数
1	ALL=((intrud* OR intrusion OR anomaly OR attack OR ((unauthori* OR unauthenticat*) ADJ5 (access OR communication)) OR malware OR ransomware OR virus OR bot OR spyware OR worm) ADJ5 (detect* OR detection OR sens*)) AND ALL=((cyber OR information OR network OR computer OR LLM OR ″Large Language Models″ OR robustness) ADJ3 (security OR attack OR intrud* OR intrusion OR adversar*)) AND (PY>=(2017) AND PY<=(2024))	18,788

検索結果の数は 18,788 件であった。

論文データの解析にあたっては、論文検索式で抽出されたすべての文献を調査者が読込み(詳細解析)を行い、技術区分表に規定された個々の技術区分への合致性を判定した。特許詳細解析と同じく本調査の対象外と判定されるものはノイズとして排除した。ノイズとして排除されなかった論文数は 16,389 件であった。

なお、論文検索式に現れる検索対象フィールドと演算子の意味は表 1-4-5 を参照されたい。

表 1-4-5 論文検索式に現れる検索対象フィールドの説明

フィールド・演算子名	意味
ALL	全文を対象に検索
ADJ5	指定した順序で 5word 以内で隣接する語句を含むレコードを検索
PY	発行年

第２章　市場環境調査

第２章では本テーマに関する市場環境調査について取りまとめている。

要約

第２章の要約

- 2019～2032 年の国・地域別市場規模を見ると、2024 年は米国・欧州・中国が市場を牽引している。CAGR(年平均成長率)ではイスラエル、韓国、日本が高く各地域で 10%超の成長が見込まれる。
- 2024 年の世界サイバーセキュリティ市場は 1,937 億米ドルであり、上位 5 社が約 42%である約 813 億米ドルを占有している。上位企業には Cisco(米国)や Palo Alto Networks(米国)が含まれておりネットワーク機器に強みを持つ企業が多い。
- 日本国内の主要セキュリティ製品市場では米国企業が約 7 割のシェアを占め、国内企業は低水準にとどまる。また、国内企業の海外売上額の大部分は MSS／MDR の売上げである。
- EDR は 2010 年代前半に登場し、他のセキュリティ製品との統合や AI 活用を通じて、高度な脅威検知能力とセキュリティ運用の効率化を実現するプラットフォームへと発展している。
- NDR は 2010 年代にネットワーク挙動の可視化を目的として登場し、クラウド環境への対応を軸に進化してきた。近年では XDR 等との連携が進み、ネットワークを含む複数領域を横断した検知・対応の自動化基盤へ発展している。
- XDR は 2010 年代に EDR の拡張として登場し、複数アセットの相関分析による検知を特徴としている。2020 年代には自動化機能や生成 AI を実装し、統合的なセキュリティ運用基盤へ進化している。
- SIEM は 2000 年代にログ集中管理と監査対応を目的として導入が進み、2010 年代には相関分析や脅威ハンティング用途へ拡張された。現在は生成 AI や SOAR と組み合わされ、SOC[3]運用の中核を担う分析・制御基盤として位置付けられている。
- SOAR は 2010 年代に SOC 業務の自動化を目的として登場し、アラート対応や封じ込めの自動化を実現した。2020 年代には SIEM や XDR と統合され、MSS／MDR における運用自動化を支える中核技術となっている。
- 脅威インテリジェンス提供サービスは 2000 年代に商用サービス化し、2010 年代に情報共有と高度分析が進展した。2020 年代にはセキュリティ製品との連携や AI 活用により、脅威の優先度判定や対応判断を自動化する役割が強まっている。
- MDR は 2010 年代に検知から対応までを含むサービスとして普及した。2020 年代には AI 活用や他サービスとの連携が進み、高度なセキュリティ運用サービスへ発展している。
- Firewall は 2010 年代にクラウド化の進展に伴い仮想型が普及した。2020 年代には AI による運用自動化やゼロトラストへの対応が進んでいる。
- Sandbox は 2000 年代に専用環境での挙動解析として登場し、2010 年代にはクラウド対応が進んだ。2020 年代には AI や機械学習を活用し、高速かつ高精度な未知脅威検知を実現している。

[3] Security Operation Center(SOC)：組織のネットワークやシステムを監視し、脅威の検知・分析・対応を行う専門組織。

第１節　調査対象となるサイバーセキュリティ市場について

１．　世界のサイバーセキュリティ市場の定義

本調査ではサイバーセキュリティ市場をネットワークや端末、クラウド環境等への不正アクセスやサイバー攻撃、システム破壊といった脅威から情報資産やシステムを保護するための製品やサービスで構成するものとする。この市場には企業の IT システム、クラウド基盤、重要インフラ、個人端末等のデジタル環境全体にわたる脅威の検知や防止、対応を支援する多様な製品やサービスが含まれる。それら製品やサービスは表 2-1-1 に示すように、ネットワーク・エンドポイント防御(Firewall/AM/AV)、侵入検知・防止システム(IDPS)、認証・アクセス管理(IAM)、情報保護・復旧対策(DLP&DR)、セキュリティ情報・イベント管理(SIEM)、その他、サービスの大きく 7 つに分類することができる。本調査対象とした EDR や Firewall、Sandbox はネットワーク・エンドポイント防御に含まれ、NDR は侵入検知・防止システムに含まれ、SIEM はセキュリティ情報・イベント管理に含まれ、MDR はサービスに含まれ、XDR、SOAR、脅威インテリジェンス提供サービスはその他に含まれる。

表 2-1-1　サイバーセキュリティ市場を構成する製品・サービスの分類と定義

セキュリティ製品及びサービス	定義
ネットワーク・エンドポイント防御 (Firewall/AM/AV)	ネットワーク・エンドポイント防御とは、ネットワーク通信および端末機器に対する不正アクセスやマルウェアの侵入を防止するための防御手段である。 具体的にFirewallやアンチマルウェア（AM）、アンチウイルス（AV）等が含まれる。Firewallはデータパケットを監視・フィルタリングし、不正アクセスを遮断する。アンチウイルスは端末上のマルウェアを検出・除去し、アンチマルウェアはシグネチャベースの検出技術を用いて悪意あるソフトウェアを識別する。
侵入検知・防止システム (IDPS)	侵入検知・防止システムとは、ネットワーク上の潜在的な脅威を監視・検出・排除することで攻撃による被害を未然に防ぐ防御手段である。 本セグメントに含まれるIntrusion Detection and Prevention System（IDPS）は、ネットワークセキュリティソリューションとして、通信を監視し、脅威を特定・排除する機能を有している。
認証・アクセス管理 (IAM)	認証・アクセス管理とは、ユーザのユーザ名やパスワード等のデジタルアイデンティティを管理し、重要情報へのアクセスを制御することで、不正利用や情報漏えいを防止する防御手段である。アイデンティティおよびアクセス管理（IAM）は、組織がデジタルアイデンティティを管理し、重要情報へのユーザーアクセスを統制するためのプロセスや技術の総称であり、これらの製品が含まれる。
情報保護・復旧対策 (DLP＆DR)	情報保護・復旧対策とは、機密情報の漏えいや損失を防止し、システム障害発生時における業務継続を確保するための防御手段である。 データ損失防止（DLP）は、機密情報の不適切または危険な転送・使用・共有を検知する。一方、災害復旧（DR）は、自然災害やシステム障害等によって情報システムやITインフラが停止した場合に、システムやデータを迅速に復旧するためのプロセスや技術である。
セキュリティ情報・イベント管理 (SIEM)	セキュリティ情報・イベント管理とは、セキュリティに関するログやイベントを一元的に収集・分析し、脅威の早期発見と対応を支援する防御手段である。 具体的にはセキュリティイベント管理（SEM）とセキュリティ情報管理（SIM）から構成され、セキュリティ脅威の特定や評価、対応を支援するソフトウェアおよびサービスである。
その他	サイバー攻撃や不正アクセスからネットワーク・データ・プログラムを守るための技術的製品群の内、主要5分類（FW～SIEM）に該当しないソリューション。 このセグメントにはSOAR、XDR、脅威インテリジェンス提供サービス等が含まれる。
サービス	セキュリティサービスは大きく、Managed Security Services（MSS）とSecurity Consulting Services（SCS）に分けられ、本セグメントにはMDRが含まれる。 Managed Security Services（MSS)は、24/7のリモート監視によるセキュリティイベントの監視、ITセキュリティ技術の管理および運用など、その他の継続的なセキュリティ対応サービスが含まれる。 Security Consulting Services（SCS）は、ITセキュリティ設計、セキュリティインフラ、組織のサイバーセキュリティ戦略の見直しに関する助言およびコンサルティング業務が含まれる。

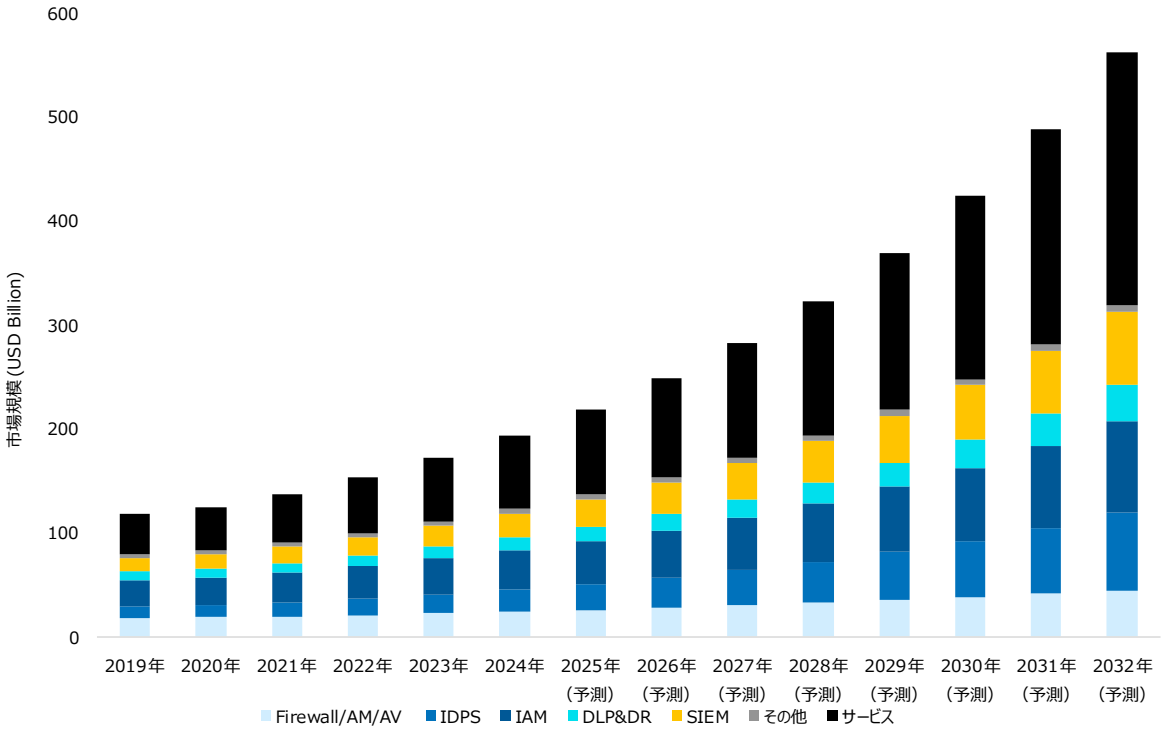
出典：Cybersecurity Market Size, Share, Analysis global report 2032(Report ID：101165) 2025 Fortune Business Insights Pvt. Ltd. p.12 Chapter 01 Definition, By Solution を参考に NTT データ経営研究所作成

２．　世界のサイバーセキュリティ市場規模・推移(ソリューション別)

1. に示したサイバーセキュリティ市場を構成する製品・サービスの総売上げを各製品・サービスの市場規模とし、図 2-1-1 と

表 2-1-2 に各種製品・サービスの市場規模の推定値と予測値を示す。2019 年から 2024 年の市場規模は推定値であり、2025 年から 2032 年までの市場規模は予測値である。製品･サービス別では MSS 等を含むサービス市場が最大であり､2024 年では 709 億米ドル、2032 年まで CAGR16.8%で拡大し 2,430 億米ドルに到達する見込みである。次点で認証・アクセス管理(IAM)市場が大きく、2024 年では 373 億米ドル、2032 年まで CAGR11.5%で拡大し 881 億米ドルに到達する見込みである。ネットワーク・エンドポイント防御(Firewall/AM/AV)市場は 2024 年では 241 億米ドル、2032 年まで CAGR8.1%で拡大し 447 億米ドルに、セキュリティ情報・イベント管理(SIEM)市場は 2024 年では 230 億米ドル、2032 年まで CAGR15.0%で拡大し 699 億米ドルに、侵入検知・防止システム(IDPS)市場は 2024 年では 216 億米ドル、2032 年まで CAGR16.9%で拡大し 747 億米ドルに、情報保護・復旧対策(DLP&DR)市場は 2024 年では 126 億米ドル、2032 年まで CAGR13.9%で拡大し 355 億米ドルに到達する見込みである。

図 2-1-1　製品・サービス別売上げに基づく市場規模推定と予測



出典：Cybersecurity Market Size, Share, Analysis global report 2032(Report ID：101165) 2025 Fortune Business Insights Pvt. Ltd. p.52 Chapter 05 Global Cybersecurity Market, By Component Global Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032 を参考に NTT データ経営研究所作成

表 2-1-2　製品・サービス別売上げに基づく市場規模推定と予測

単位 USD Billion	年														CAGR 2025-2032
	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	
	推定値						予測値								
Firewall/AM/AV	18.3	18.6	19.6	21.0	22.5	24.1	25.9	27.9	30.1	32.5	35.2	38.2	41.4	44.7	8.1%
IDPS	11.1	12.2	13.9	16.1	18.6	21.6	25.1	29.2	34.0	39.6	46.3	54.4	63.7	74.7	16.9%
IAM	25.5	26.4	28.4	31.0	34.0	37.3	41.1	45.5	50.4	56.1	62.6	70.1	78.6	88.1	11.5%
DLP&DR	7.8	8.2	9.0	10.1	11.3	12.6	14.2	16.1	18.2	20.7	23.6	27.0	30.9	35.5	13.9%
SIEM	13.3	14.3	15.9	18.0	20.3	23.0	26.2	29.9	34.3	39.3	45.3	52.3	60.5	69.9	15.0%
その他	3.5	3.5	3.6	3.8	4.0	4.2	4.5	4.7	5.0	5.3	5.6	5.9	6.1	6.4	5.2%
サービス	38.5	41.6	46.9	53.7	61.6	70.9	82.0	95.0	110	129	150	177	207	243	16.8%
Total	117	124	137	153	172	193	218	248	282	322	368	424	488	562	14.4%

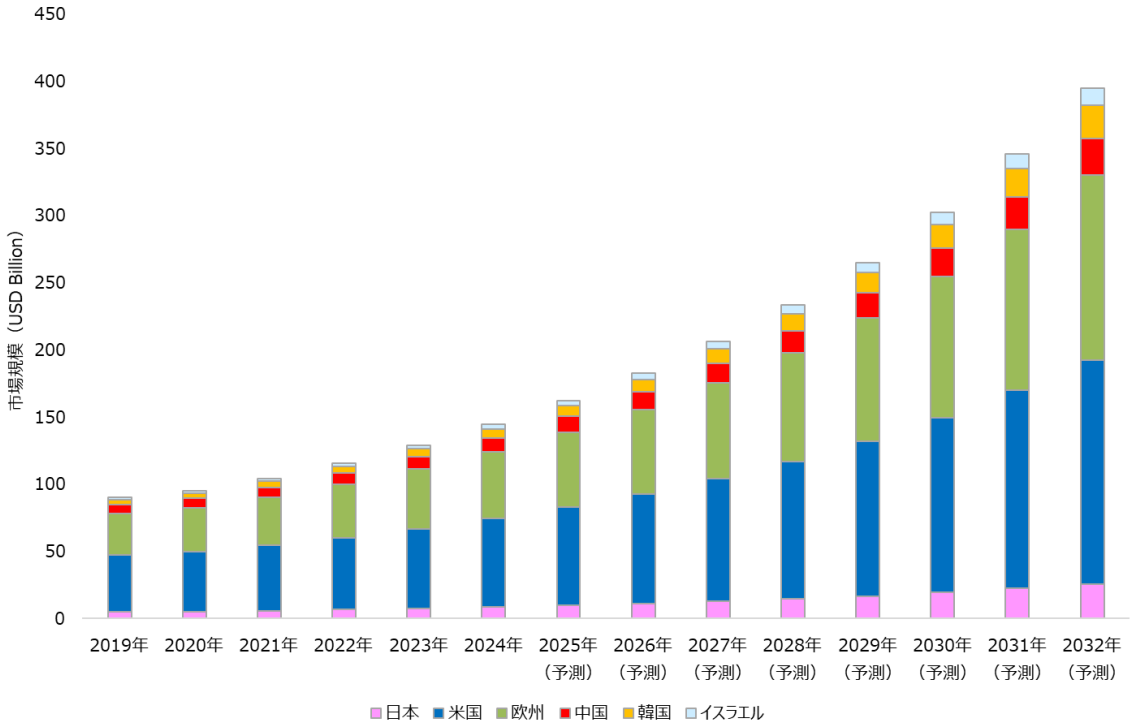
出典：Cybersecurity Market Size, Share, Analysis global report 2032(Report ID：101165) 2025 Fortune Business Insights Pvt. Ltd. p.52 Chapter 05 Global Cybersecurity Market, By Component Global Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032 を参考に NTT データ経営研究所作成

３．　世界のサイバーセキュリティ市場規模・推移(国・地域別)

1. に示したサイバーセキュリティ市場を構成するソリューションの総売上げをサイバーセキュリティ市場の市場規模とし、日本、米国、欧州、中国、韓国、イスラエルの国・地域別のサイバーセキュリティ市場規模の推定値と予測値(2019 年から 2032 年まで)、2025 年から 2032 年にかけての CAGR を共に図 2-1-2 と表 2-1-3 に示す。2019 年から 2024 年までの市場規模は推定値であり、2025 年から 2032 年までの市場規模は予測値である。

2024 年日本のサイバーセキュリティ市場は 86 億米ドル、米国市場は 657 億米ドル、欧州市場は 498 億米ドル、中国市場は 104 億米ドル、韓国市場は 68 億米ドル、イスラエル市場は 32 億米ドルである。市場規模の観点では米国、欧州、中国市場がサイバーセキュリティ市場全体を牽引しており、最大の市場規模を誇る米国市場は 2032 年までに 1,670 億米ドルまで拡大する見込みである。一方で 2025 年から 2032 年までの CAGR に着目すると、日本市場は 15.0%、米国市場は 12.5%、欧州市場は 13.7%、中国市場は 13.1%、韓国市場は 17.5%、イスラエル市場は 19.5%である。イスラエル市場の成長率が一番高く、次点で韓国市場、日本市場の成長率が高い。各国・地域の CAGR が 10%以上であることを踏まえ、サイバーセキュリティ市場は引き続き拡大傾向にあると予測される。

図 2-1-2　製品・サービスの売上げに基づく国・地域別のサイバーセキュリティ市場規模推定と予測



出典：Cybersecurity Market Size, Share, Analysis global report 2032(Report ID：101165) 2025 Fortune Business Insights Pvt. Ltd. p.72 Chapter 06 North America Cybersecurity Market, By Country, North America Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032, p.94 Chapter 08 Europe Cybersecurity Market, By Component, Europe Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032, p.105 Chapter 09 Middle East & Africa Cybersecurity Market, By Country, Middle East & Africa Cybersecurity Market Estimates and Forecast (USD Bn), By Country, 2019-2032, p.116 Chapter 10 Asia Pacific Cybersecurity Market, By Component, Asia Pacific Cybersecurity Market Estimates and Forecast (USD Bn), By Country, 2019-2032 を参考に NTT データ経営研究所作成

表 2-1-3　製品・サービスの売上げに基づく国・地域別のサイバーセキュリティ市場規模推定と予測

単位 USD Billion	年														CAGR 2025-2032
	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	
	推定値						予測値								
日本	5.1	5.4	5.9	6.7	7.6	8.6	9.8	11.1	12.7	14.6	16.8	19.4	22.4	25.9	15.0%
米国	42.3	44.7	48.6	53.6	59.3	65.7	73.1	81.6	91.3	102	115	130	147	167	12.5%
欧州	30.8	32.6	35.7	39.8	44.5	49.8	56.0	63.1	71.3	80.9	92.0	105	120	137	13.7%
中国	6.6	6.8	7.5	8.3	9.3	10.4	11.6	13.0	14.7	16.6	18.7	21.3	24.2	27.4	13.1%
韓国	3.6	3.9	4.4	5.1	5.9	6.8	7.9	9.2	10.8	12.7	14.9	17.6	20.8	24.5	17.5%
イスラエル	1.6	1.8	2.0	2.3	2.7	3.2	3.8	4.5	5.3	6.3	7.6	9.1	10.9	13.1	19.5%

出典：Cybersecurity Market Size, Share, Analysis global report 2032(Report ID：101165) 2025 Fortune Business Insights Pvt. Ltd. p.72 Chapter 06 North America Cybersecurity Market, By Country, North America Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032, p.94 Chapter 08 Europe Cybersecurity Market, By Component, Europe Cybersecurity Market Estimates and Forecast (USD Bn), By Component, 2019-2032, p.105 Chapter 09 Middle East & Africa Cybersecurity Market, By Country, Middle East & Africa Cybersecurity Market Estimates and Forecast (USD Bn), By Country, 2019-2032, p.116 Chapter 10 Asia Pacific Cybersecurity Market, By Component, Asia Pacific Cybersecurity Market Estimates and Forecast (USD Bn), By Country, 2019-2032 を参考に NTT データ経営研究所作成

第２節　世界のサイバーセキュリティ市場シェア

第１節１．に示したサイバーセキュリティ市場の定義に従い、世界のサイバーセキュリティ市場の主要プレイヤを表 2-2-1 に、各プレイヤの市場シェアを図 2-2-1 に示す。セキュリティ製品・サービスの売上げが高い企業や、ある特定の製品領域に特化している企業を網羅的に抽出するため、市場を構成する企業を、上位 5 社、領域特化型、その他の 3 つの企業群に分類する。上位 5 社は 2024 年サイバーセキュリティに関するグローバル売上げ上位 5 社と定義する。領域特化型は、複数領域の製品やサービスをグローバルに提供しており、その中でもある特定領域に専門性や技術的差別化要素を有する企業、その他は上位 5 社、領域特化型に含まれない企業と定義する。その他の主要企業として列挙した企業は、単一の国や地域での事業展開、特定製品カテゴリの提供等により、上位 5 社や領域特化型と比較し、売上げシェアが低い点が特徴である。具体的に上位 5 社には Cisco Systems(米国)や Palo Alto Networks(米国)が、領域特化型には NTT データ(日本)や Broadcom(米国)、その他には Sophos(英国)や Trend Micro(日本)等が含まれる。

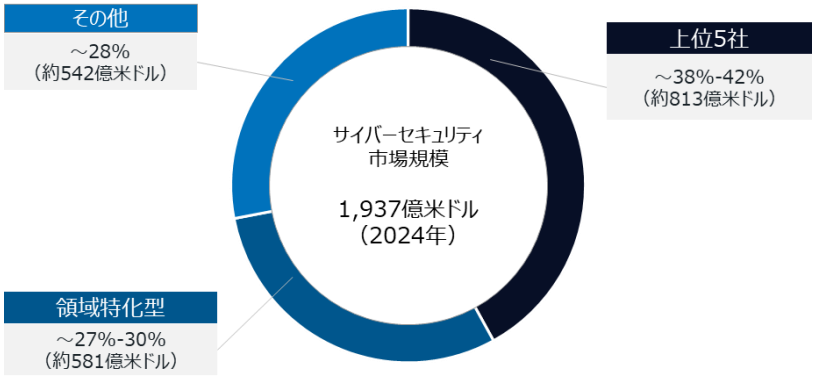
2024 年、世界のサイバーセキュリティ市場規模は 1,937 億米ドルであり、そのうち上位 5 社の企業によって市場の約 42%である約 813 億米ドルが占有されている。また、領域特化型の企業によって約 30%である約 581 億米ドルが、その他の企業によって約 28%である約 542 億米ドルが占有されている。上位 5 社の企業に Cisco Systems(米国)や Palo Alto Networks(米国)が含まれていることから、世界のサイバーセキュリティ市場シェアの上位を占める企業はネットワーク機器に強みを持っている企業が多い傾向にある。

表 2-2-1　世界のサイバーセキュリティ市場を構成する企業群

	上位5社	領域特化型	その他
定義	• 2024年サイバーセキュリティに関するグローバル売上上位5社	• 複数領域の製品やサービスをグローバルに提供しており、その中でもある特定領域に専門性や技術的差別化要素を有する企業	• 上位5社、領域特化型に含まれない企業
主要企業	• IBM Corporation • Fortinet, Inc. • Palo Alto Networks, Inc. • Microsoft Corporation • Cisco Systems Inc.	• NTT Data • Broadcom • F5 Networks • Check Point Software Technologies • Zscaler • Juniper Networks • Proofpoint • CrowdStrike Holdings • Cloudflare	• Sophos Ltd. • Amazon Web Services • McAfee • LLC • Trend Micro • Cynet • Micro Focus • Imperva • T-Mobile USA • Alphabet • Others
市場シェア	• 世界のサイバーセキュリティ市場の約38～42%を5社で占有	• 世界のサイバーセキュリティ市場の約27～30%をこの企業群で占有	• 世界のサイバーセキュリティ市場の約28%をこの企業群で占有

出典：Cybersecurity Market Size, Share, Analysis global report 2032（Report ID：101165）2025 Fortune Business Insights Pvt. Ltd. p.47 Chapter 04 Global Cybersecurity Key Players' Market Share Analysis, 2024 を参考に NTT データ経営研究所作成

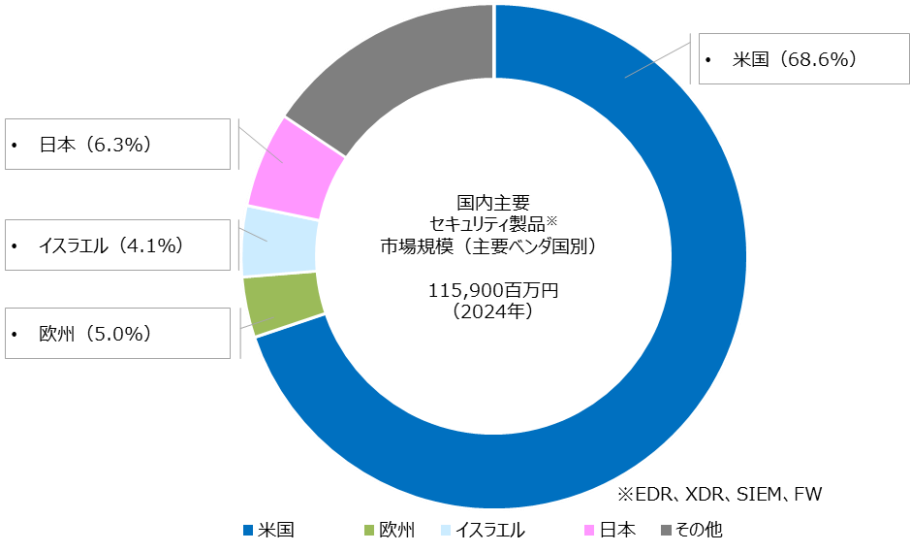
図 2-2-1　世界のサイバーセキュリティ市場を構成する企業群の市場シェア



出典：Cybersecurity Market Size, Share, Analysis global report 2032（Report ID：101165）2025 Fortune Business Insights Pvt. Ltd. p.47 Chapter 04 Global Cybersecurity Key Players' Market Share Analysis, 2024 を参考に NTT データ経営研究所作成

図 2-2-2 に 2023 年度日本国内の主要なサイバーセキュリティ製品（EDR、XDR、SIEM、Firewall）の市場規模と内訳を示す。米国企業が日本の国内シェアの 68.6%と過半数を占めているのに対して、国内企業は 6.3%にとどまっている。国別の主要企業を見ると、先行してグローバルで市場開拓を進め、政府・大企業での採用実績が多い企業がシェアを獲得していることが分かる。ネットワーク、Firewall、EDR 等、企業の主要なセキュリティアーキテクチャを提供する製品群が日本で市場シェアを獲得している。また、国内企業の海外売上額の大部分は MSS／MDR の売上げである。

図 2-2-2　国内主要セキュリティ製品市場規模(主要ベンダ国別)



出典：富士キメラ総研 2024 ネットワークセキュリティビジネス調査総覧＜市場編＞ 2024 年 12 月 19 日 株式会社富士キメラ総研／第三部 p.195 2-20.EDR 5.市場占有率推移、p.222 2-26.XDR 5.市場占有率推移、p.218 2-25.統合ログ管理ツール(SIM/SIEM) 5.市場占有率推移、p.127 2-4.ファイアウォール/VPN/UTM 関連製品 5.市場占有率推移を参考に NTT データ経営研究所作成

第３節　主要企業動向・製品動向

１．　EDR 製品に関する製品の一覧及びその年代ごとの推移

表 2-3-1 に 2010 年代から 2020 年代までの EDR の変遷を示す[4,5]。

2010 年代前半には、従来のアンチウイルス(AV)が未知のマルウェアやファイルレス攻撃を検知できず、標的型攻撃の挙動の追跡にも対応困難であることが明らかとなり、端末での異常挙動検知とマルウェア除去・封じ込めを備えた EDR が登場した。最初にシェアを拡大した Carbon Black EDR は端末の全アクティビティをクラウド上で継続記録し、攻撃の一連のキルチェーンをコンソール上で可視化した上で遠隔で端末の遮断及び復旧を実現した。2011 年～2014 年にかけて CrowdStrike は Falcon Insight でクラウド管理の軽量センサを展開し、IoC や IoA に基づく振る舞い検知とリアルタイムハンティングを普及させた。

2010 年代後半は、マルウェアの攻撃が高速化・複雑化したことに加えて、企業のセキュリティ対策が進んだ結果、対処すべきセキュリティ業務が増大し、セキュリティアナリスト不足が顕在化するようになった。これにより EDR には異常検知だけでなく、自動修復機能によってマルウェアに感染した端末を即座に遮断する役割が求められるようになった。Windows Defender ATP は OS に統合された EDR として、振る舞い検知や IoC 収集の機能を提供し、Defender Suite 内のセキュリティ製品との連携により分析能力が向上した。Symantec EDR はワンクリックによる端末隔離や高速な修復を強みに、インシデント初動対応の自動化を強調した。これらの動きに象徴されるように、2010 年代後半は各社がセキュリティ機能の統合と運用自動化を軸に差別化を図っていたと推測される。

[4] Palo Alto Networks(https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr)
[5] Gartner「Magic Quadrant for Endpoint Protection Platforms」

2020 年代は、EDR 以外のセンサ製品を統合した XDR と AI による自動防御が拡大した。Microsoft Defender XDR/Defender for Endpoint は、Microsoft のセキュリティ製品を横断して取得したログを相関分析し、進行中の攻撃を高信頼で検知・遮断・自動修復する機能を搭載した。また、Trellix EDR は AI を用いてアラートと攻撃 TTP を過去データと相関分析することで、攻撃の経路を可視化して原因を迅速に解明できるよう設計されている。

2010 年代に未知の脅威対策として登場した EDR は、他のセキュリティ製品との統合や AI 活用を通じて、高度な脅威検知能力とセキュリティ運用の効率化を実現するプラットフォームへと発展している。

表 2-3-1　2010 年代から 2020 年代までの EDR の変遷

	2010年代前半	2010年代後半	2020年代
主要企業	クラウド常時監視型EDR製品の登場	自動修復と調査ガイド普及	XDR統合＋AI自動防御の拡大
CrowdStrike（米国）	**Falcon** • 2013年にリリース。クラウド基盤で監視対象のエンドポイントをリアルタイムに監視し、IoAを基にした攻撃行動検知とMITERATT&CKマッピングによって攻撃の可視化・インシデント対応を高速化。	**Falcon（機能拡張）** • Firewall Management等のモジュールを追加することでクラウド基盤の検知・追跡性能を強化。	**Falcon Insight** • 2022年にリリース。XDRとの統合によってEDRだけでなく他製品からのテレメトリを相関分析し、脅威情報の調査やインシデントレスポンスまでを自動化。
Microsoft（米国）		**Windows Defender ATP** • Windows 10の内蔵センサーで侵害検知・調査・応答を提供。2019年にMac対応も開始。	**Microsoft Defender for Endpoint** • 2020年に名称を変更。エンドポイントの脆弱性管理、次世代AV、EDR、自動インシデントレスポンスを単一プラットフォームで提供。
Cisco Systems（米国）	**FireAMP** • 2012年にリリースされ、クラウドによるファイル奇跡の分析、遡及検知によってエンドポイントの異常挙動を可視化。	**AMP for Endpoints** • EPPとEDRを兼ね備えたソリューションとして提供。Ciscoのファイアウォール製品やメールセキュリティ製品などと連携し、ブラックリストを共有。	**Cisco Secure Endpoint** • エンドポイントの状態をリアルタイムで取得し、Ciscoの脅威インテリジェンスサービスであるTalosと連携したマルウェアの封じ込め・除去を高速で実行することが可能。
Check Point Software Technologies（イスラエル）		**SandBlast Agent** • 2019年にリリースされ、機械学習による行動分析・マルウェアの無害化によってエンドポイントにおけるセキュリティを向上。	**Harmony Endpoint** • SandBlastを改称。取得ファイル無害化とサンドボックス環境での解析を並行して実行する点に特徴がある。
Fortinet（米国）			**FortiEDR** • 2019年にenSiloを買収することでEDR技術を獲得し、2020年代にFortinet Security Fabricのエンドポイント対策製品としてリリース。Fortinet製品や脅威インテリジェンスサービス「FortiGate」との連携に強み。
Broadcom（米国）	**Carbon Black EDR** • 2011年にリリースされ、端末のアクティビティを持続的に記録し、キルチェーンを可視化。リアルタイムハンティングと遠隔復旧を実現。	**Symantec EDR** • 従来のEPP製品にEDR機能を統合。脅威インテリジェンス情報によって脅威検知性能を強化。	**Symantec Endpoint Security/VMware Carbon Black** • Broadcomが2019年にSymantec Enterpriseを取得、2023年にVMware買収完了。以降はSymantec EnterpriseとCarbon Black Cloudの両系を展開。
Trellix（米国）		**McAfee Active Response/Fire Eye Endpoint Security** • TrellixのEDR製品の前身としてMcAfeeとFireEyeから提供。	**Trellix Endpoint Detection and Respons** • McAfee Enterprise＋FireEyeの統合ブランドとしてEDR/XDRを提供。検知直後に対象端末の情報を取得しフォレンジックを実行する機能を標準搭載。

2．　NDR 製品に関する製品の一覧及びその年代ごとの推移

NDR 製品は 2010 年代から登場したため、2010 年代から 2020 年代にかけての NDR の変遷を表 2-3-2 に示す。

2010 年代は、NDR が登場し、クラウド環境への適応が進展した時期である。Cisco Systems は 2017 年に Observable Networks を買収し、Stealthwatch(現在の Cisco Secure Network Analytics)をクラウド対応に拡張[6]した。Darktrace は 2018 年に Darktrace Cloud

[6] Cisco Systems(https://blogs.cisco.com/news/cisco-announces-cloud-security-news)

を発表し、クラウド環境向けのセキュリティ機能を強化[7]した。Palo Alto Networks は 2019 年に Cortex XDR を提供開始し、ネットワーク、エンドポイント、クラウドを統合的に監視する仕組みを実現[8]した。Trend Micro は Trend Micro Cloud Network Protection を発表し、クラウド保護機能を強化[9]した。

2020 年代に入ると、クラウド環境への拡大とともに、プラットフォームや XDR との連携が加速した。Cisco Systems は Cisco XDR を展開し、Microsoft や Darktrace のセキュリティデータと連携することで、検知から対応までの自動化を実現[10]した。Darktrace は ActiveAI Security Platform を発表[11]し、NDR 製品 Darktrace/NETWORK と XDR を統合した防御体制を構築した。Palo Alto Networks は Cortex XDR を強化し、複数の情報技術と連携しながら包括的な脅威対策を提供[12]している。Trend Micro は Trend Vision One を基盤に、メール、エンドポイント、クラウド、ネットワークを横断的に監視する体制を整備[13]した。このように、NDR はクラウド対応を起点に、XDR や各種プラットフォームとの統合を図っている。

[7] Darktrace(https://www.darktrace.com/news/darktrace-cloud-protects-next-wave-of-cloud-computing-models-and-more-saas-applications)
[8] Palo Alto Networks(https://www.paloaltonetworks.ca/company/press/2019/palo-alto-networks-introduces-cortex-the-industrys-only-open-and-integrated-ai-based-continuous-security-platform)
[9] Trend Micro(https://www.trendmicro.com/en/about/newsroom/local-press-releases/hk/2019/2019-07-12.html)
[10] Cisco Systems(https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m04/cisco-unveils-new-solution-to-rapidly-detect-advanced-cyber-threats-and-automate-response.html)
[11] PR Newswire(https://www.prnewswire.com/news-releases/darktrace-transforms-security-operations-and-improves-cyber-resilience-with-launch-of-darktrace-activeai-security-platform-302111097.html)
[12] Palo Alto Networks(https://www.paloaltonetworks.jp/company/press/2021/palo-alto-networks-launches-cortex-xdr-for-cloud--xdr-3-0-expands-industry-leading-extended-detection-and-response-platform-to-cloud-and-identity-to-detect-and-stop-cyberattacks)
[13] Trend Micro(https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210312-01.html)

表 2-3-2　2010 年代から 2020 年代までの NDR の変遷

	2000年代	2010年代	2020年代
主要企業		クラウド環境への対応	XDR・プラットフォームとの連携
Cisco Systems（米国）		**Stealthwatch（現在のCisco Secure Network Analytics）をクラウド環境に対応させる** • 2017年に、クラウドベースのセキュリティサービスを提供するObservable Networksを買収することにより、自社NDR製品のStealthwatchをクラウド環境に対応させた。	**Cisco XDR** • 2023年に、ネットワークやエンドポイント等から脅威を検知・分析するCisco XDRを発表。CrowdStrikeやMicrosoft、Darktraceのセキュリティ製品とデータを連携。
Darktrace（英国）		**Darktrace Cloud** • 2016年に、クラウド環境に対応したセキュリティ製品であるDarktrace Cloudを発表。	**Darktrace ActiveAI Security Platform** • 2024年に、DarktraceのNDR製品であるDarktrace/NETWORK等と連携したプラットフォームであるDarktrace ActiveAI Security Platformを発表。
Palo Alto Networks（米国）		**Cortex XDR** • 2019年に、ネットワークやエンドポイント、クラウドデータを統合するセキュリティプラットフォームであるCortex XDRを発表。	**Cortex XDR** • 2021年に、Palo Alto NetworksはCortex XDRのユーザ行動分析機能をさらに強化し、広範囲のIDデータを収集・分析することが可能となった。
Trend Micro（日本）		**Trend Micro Cloud Network Protection** • 2019年に、Trend Microはネットワークセキュリティをクラウド環境に拡張したTrend Micro Cloud Network Protectionを発表。	**Trend Micro Vision One** • 2021年に、ネットワークやエンドポイント、クラウド等を分析し、攻撃の全体像を可視化するプラットフォームであるTrend Micro Vision Oneを発表。
Vectra AI（米国）		**Cognito platform** • 2018年に、クラウド環境上の脅威を検知を強化するために、Microsoft Azureとの統合を行い、Azure Virtual Network Terminal Access Pointを通過する全てのトラフィックを監視。	**Vectra AI Platform** • 2023年に、ネットワークやクラウド、ID等のシグナルをエンドポイントのシグナルと統合するプラットフォームであるVectra AI Platformを発表。

3．　XDR 製品に関する製品の一覧及びその年代ごとの推移

XDR 製品は 2010 年代から登場したため、2010 年代から 2020 年代にかけての XDR の変遷を表 2-3-3 に示す。

エンドポイントセキュリティのトレンドとして、2010 年代は EDR による未知の脅威に対する検知・対処の仕組みが普及した。その後、クラウド基盤利用の拡大や、ゼロトラスト・セキュリティの普及によって、より広範囲のアセットへの対策が求められるようになった。具体的には、ID の不正利用やフィッシングメール経由の侵入、クラウド設定不備を突いた攻撃等の異常を検知するために、単一のアセットやツールのログだけでなく、系全体の動向を相関分析することで精度の高い検知が可能となった。各企業の動向として、2019 年に Palo Alto Networks[14]、Trend Micro[15]が XDR をリリースし、XDR の市場展開が進んだ。主要ベンダの市場参入を契機となり、企業に導入されるセキュリティソリューションが EDR から、XDR のように横断的に多様な ICT 機器を検知対象とするソリューションに変化し始めた。

2020 年代は、コロナ禍を契機に企業の ICT 環境が大きく変化しクラウドサービスの利用が拡大した。従来の IT 環境では全ての機器のログやイベントを把握することが困難となった。加えて SOC 業務担当、特にセキュリティアナリストが減少傾向で、少人数で膨大なアラートに対処しなければならなくなった。こうした背景から、より少ない人員で効率的に分析や調査を行えるよう、アナリストの業務を効率化・自動化できるよう機能の高度化も進められてきた。

2020 年代中盤には、生成 AI 技術がセキュリティ分野にも拡大し、CrowdStrike は、独

[14] Palo Alto Networks(https://www.paloaltonetworks.com/company/press/2019/palo-alto-networks-introduces-cortex-the-industrys-only-open-and-integrated-ai-based-continuous-security-platform)
[15] Trend Micro(https://newsroom.trendmicro.com/2019-11-18-Trend-Micro-Debuts-Worlds-Broadest-Security-Services-Platform-for-Organizations-Building-Applications-in-the-Cloud)

自の生成 AI である Charlotte AI を自社の XDR 製品へ組み込み[16]、自然言語を用いた調査分析の機能を実現した。

このように XDR は EDR の範囲の拡張・高度化が進み、横断的なログ分析や、インシデント対応の自動化機能を取り込みつつある。XDR は単なる検知製品から、企業全体のセキュリティ運用を統合的に支える製品へと進化している。

表 2-3-3　2010 年代から 2020 年代までの XDR の変遷

	2000年代	2010年代	2020年代
主要企業		各ツールの統合・XDRの登場	AIの活用・運用効率化
CrowdStrike（米国）		**CrowdStrike falcon platform** • エンドポイントやクラウド、ID等の広範な領域に対するCrowdStrikeのソリューションを単一のプラットフォームで提供し、1つのコンソールで全機能の管理が可能。	**Falcon XDR** • 2022年に、Falcon XDRを発表。ネットワーク、Web、クラウド等のサードパーティデータをCrowdStrike独自クラウドと相関させ、リアルタイム検出を実現。アラート優先度付け機能等を標準搭載し、検知から自動対応までを一元管理。
Microsoft（米国）		**Microsoft Threat Protection** • Azure ADを基盤とし、Defender ATP、Defender for Office 365、Azure ATP、Cloud App Securityを統合し一体的な脅威検出・保護を強化。	**Microsoft Defender XDR** • 2023年にMicrosoft Security Copilotを導入。自然言語インターフェースでインシデント要約やレスポンス提案によりDefender XDRを強化。
Palo Alto Networks（米国）		**Cortex XDR** • 2019年に、エンドポイントやネットワークのログを統合し、相関分析で脅威を検出するXDRプラットフォームであるCortex XDRを発表。	**Cortex XDR** • AIにより脅威の検知速度を上昇させるとともに、2024年にはMITRE ATT&CK評価で100% の検知率を達成している。
Sophos（英国）		**Sophos Central** • 2015年に、エンドポイント、サーバ、電子メール等のセキュリティを一元管理可能なクラウドベースのプラットフォームを発表。 • 2018年に、Sophos CentralにSophos XG Firewallを統合可能にした。	**Sophos XDR** • 2024年に、生成AI機能を発表。自然言語を用いて大量のセキュリティデータを検索可能とすることで、アナリストの負担を軽減。また、検知した内容を要約し、次に取るべき行動をアナリストに提案することも可能。
Trend Micro（日本）		**Trend Micro Cloud One** • 2019年に、クラウド上でアプリケーションを構築する組織向けのセキュリティプラットフォームであるTrend Micro Cloud Oneを発表。	**Trend Micro Vision One** • 2023年に、Trend Vision OneにGPTベースのアシスタント「Companion」を導入。自然言語で質問できるAIアシスタントで、セキュリティ運用を支援。

4．　SIEM 製品に関する製品の一覧及びその年代ごとの推移

表 2-3-4 に 2000 年代から 2020 年代までの SIEM の変遷を示す[17,18]。

2000 年代は、米国での企業不祥事や不正アクセス事件の増加によって企業の内部統制や透明性を担保する仕組みが不十分であることが問題視され、監査対応においてシステムの利用状況やアクセスの証跡を残すことが求められるようになった。また、IT インフラの拡大によってログの量と種類が増加したことで、複数のシステムからのログを収集し一元的に管理することが求められた。これによりセキュリティログが一元的に保管され、必要に応じて迅速に検索できる SIEM が注目され、規制遵守やインシデント発生時の監査対応に活用された。初期の SIEM はアプライアンス型で提供され、サーバやネットワーク機器からのログを収集及び一元管理したのち、アラート発報、ダッシュボード表示、報告書作成する機能が標準搭載された。

2010 年代前半は、クラウドサービスの利用が拡大し監視対象や取り扱うデータ量が更に増加した。また、サイバー攻撃も複雑化・高速化したため従来のルールベースでの攻撃検知ソリューションでは未知の攻撃や異常挙動を検知しきれないケースが増えた。こ

[16] CrowdStrike(https://www.crowdstrike.com/ja-jp/press-releases/crowdstrike-introduces-next-generation-of-the-crowdstrike-falcon-platform/)
[17] Elastic(https://www.elastic.co/jp/blog/generative-ai-revolution-in-siem)
[18] Gartner「Magic Quadrant for Security Information and Event Management」

のため、ネットワーク、Firewall、認証ログ等、複数のログソースを相関分析することで単独のソースでは見えなかった攻撃の兆候を検出する分析機能が SIEM に搭載されるようになった。2012 年には Splunk Enterprise Security が登場し、SIEM による検索・可視化基盤を活かした検知ルール運用と自動レポート作成によって組織のセキュリティ運用を強化した。これまでの監査対応中心の用途から脅威ハンティングへの活用が広がった。

2010 年代後半から 2020 年代は、ランサムウェア、ゼロデイ攻撃、サプライチェーン攻撃等、攻撃のスピードや複雑性がさらに増大したことに加えて、SOC の人材不足やスキルギャップが顕在化し誤検知・過検知によるアナリストの疲弊が問題視されるようになった。このような課題を受けて AI や機械学習を活用したログ分析の高度化やオートメーションのニーズが高まり、UEBA、SOAR、生成 AI 等が SIEM と統合されるようになった。Sumo Logic は 2018 年に Cloud SIEM を発表し、SaaS でのリアルタイム相関と UEBA を活用しノイズを抑制した。2019 年には Microsoft が Sentinel をリリースし、クラウド上で SOAR や脅威情報と連携した運用を実現した。

2000 年代に監査対応の目的で登場した SIEM は、SOC 人材不足や高度化する攻撃への対処に活用されるようになった。SIEM は、ログ管理だけでなく統合的な脅威検知・インシデント対応を行うログ管理基盤へと進化し、セキュリティ運用の中核として位置付けられている。

表 2-3-4　2000 年代から 2020 年代までの SIEM の変遷

	2000年代	2010年代前半	2010年代後半～2020年代
主要企業	オンプレでのログ収集・相関分析	クラウド・オンプレのハイブリッド化	クラウドネイティブとAI活用
Cisco Systems（米国）	**Cisco MARS** • アプライアンス型SIEMとして相関分析とレポート作成機能を提供。2011年に販売終了となった。	**Splunk Enterprise Security** • 2012年にSplunkからv5.0がリリース。大規模ログ検索エンジンを基盤として本格的にSIEM市場に参入。2016年には機械学習を組み込みUEBA機能を強化。	**Splunk Enterprise Security** • 2024年にCiscoによってSplunkを買収。RBAや相関検索、MITRE対応でSOC運用を強化。
Microsoft（米国）		**Azure Sentinel** • 2019年にクラウドネイティブSIEM/SOARとしてリリース。豊富な外部連携コネクタと機械学習ベースの行動分析に強みを持つ。	**Microsoft Sentinel** • 2022年に製品名をMicrosoft Sentinelに変更しマルチクラウド・ハイブリッドクラウド対応機能を拡張。行動分析機能も強化。
Exabeam（米国）		**Security Intelligence Platform** • 2017年にUEBAを中核機能としてリリース。ログを時系列分析することでインシデントの全体像を即座に把握可能。	**LogRhythmSIEM/Exabeam Fusion SIEM** • 2021年にリリースされ、クラウドデータレイクに蓄積された大量ログを機械学習によって解析し、関連イベントを自動時系列化。SOAR統合によってレスポンスまで対応。
Fortinet（米国）		**FortiSIEM** • 2016年にAccelOpsを買収し製品化。分散リアルタイム相関、マルチテナント対応、構成管理データベース構築で大規模なセキュリティ運用に対応。	**FortiSIEM（機能拡張）** • 機械学習による行動分析の強化や、脅威インテリジェンス情報との連携によって脅威検知の性能を向上。
Google（米国）		**Chronicle** • 2019年にGoogle Cloudに拡充された大規模セキュリティログ分析基盤。長期間のログ保管や高速検索機能に強みを持つ。	**Google Security Operations** • 2024年にGoogle Security Operationsに改称。Mandiant等の脅威インテリジェンス情報との連携によって検知からインシデント対応までを一貫して実行可能。

５． SOAR 製品に関する製品の一覧及びその年代ごとの推移

表 2-3-5 に 2010 年代から 2020 年代までの SOAR の変遷を示す[19,20]。

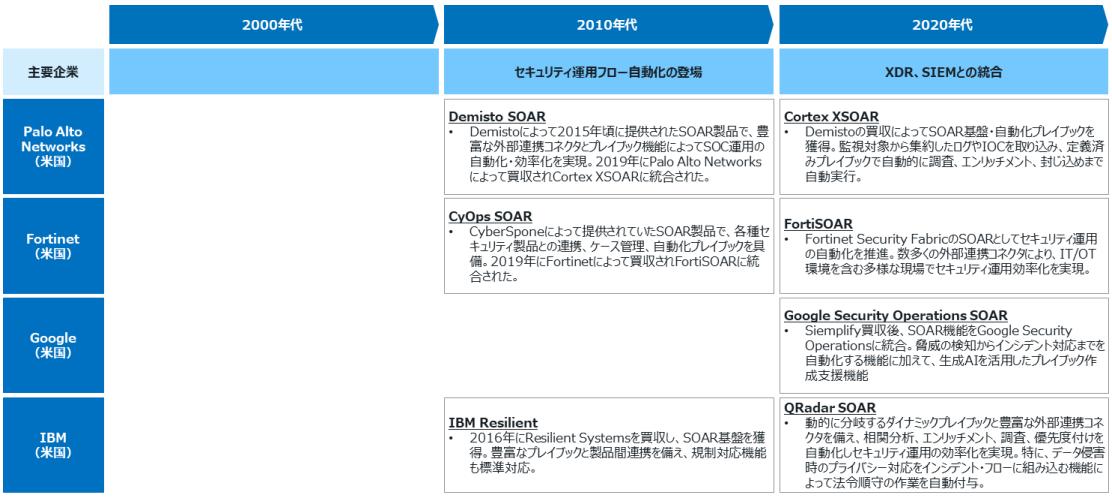
2010 年代前半頃からサイバー攻撃の高度化・多様化によって企業の SOC には膨大なアラートが集中するようになったため、SOC アナリストの業務負荷増大が課題視され始めた。また、EDR や脅威インテリジェンス提供サービス等、新たなセキュリティ製品の導入が進む中、セキュリティ製品群を統合的に活用しインシデント対応を行っていく必要性が出てきた。このような背景から 2015 年頃に、セキュリティ製品群からのアラートを集約しインシデント管理を行う機能や、脅威の調査や封じ込め作業を自動化する機能を具備した SOAR が登場した。初期の SOAR 製品は Demisto(2019 年に Palo Alto Networks によって買収)や Phantom Cyber(2018 年に Splunk によって買収)等が販売したものが代表的であり、脅威インテリジェンス情報連携による IoC 照合作業や EDR 連携による端末隔離等、これまで手動で行われてきた SOC 業務をプレイブックによって自動化した。

2020 年代になるとクラウドサービスの利用拡大やリモートワークの普及等によって監視対象が増大した。一方で、企業のガバナンス向上の観点でサイバー攻撃への対応スピード向上が求められるようになり、少ないリソースで多くのセキュリティ業務に対処することが求められるようになった。これに伴い、SOAR には自動化だけでなく脅威インテリジェンス情報や生成 AI の活用によるインシデント対応の高度化に資する機能が搭載され始めた。実際の製品としては、SOAR 単独の導入よりも SIEM や XDR に SOAR 機能を統合する形が主流となり、Cortex XSOAR、IBM QRadar SOAR、Microsoft Sentinel、Google Chronicle SOAR 等、大手ベンダのプラットフォームに組み込まれていった。また、プレイブック構築においてはノーコード・ローコードによる操作性が強化され、アナリストが容易に自動化ワークフローを設計できるよう進化した。さらに、MSS／MDR サービスにおいて SOAR が不可欠な自動化基盤として採用され、サービスベンダは複数顧客環境を横断して運用効率を改善するために SOAR を活用している。

SOAR は 2010 年代に SOC 業務の効率化を目的とした自動化ツールとして登場し、2020 年代には SIEM や XDR への統合、MSS／MDR 基盤としての普及を通じて、セキュリティ運用全体の中核機能へと進化した。

[19] Palo Alto Networks(https://www.paloaltonetworks.com/cortex/xsoar-state-of-soar-report-2020)
[20] Gartner「Hype Cycle for Security Operations, 2024」

表 2-3-5　2010 年代から 2020 年代までの SOAR の変遷



6．　脅威インテリジェンス提供サービスに関する製品の一覧及びその年代ごとの推移

表 2-3-6 に、2000 年代から 2020 年代までの脅威インテリジェンス提供サービスの変遷を示す。

2000 年代は、脅威インテリジェンス情報の提供がサービス化した年である。例えば 2003 年に、Cisco Systems はデバイスセンサからテレメトリデータを収集し、脆弱性やマルウェアの侵入経路等の情報の提供を開始した。2006 年に IBM は、脅威インテリジェンス情報の分析集団を有する Internet Security Systems[21]を買収し、Cisco Systems や Fortinet に続き攻撃動向レポート等の提供を開始する等、2000 年代は、各社が脅威インテリジェンス情報の提供をサービスとして開始し市場が形成された。

2010 年代は、脅威インテリジェンス情報の共有が加速し、分析が高度化した年である。例えば 2013 年に CrowdStrike は、パソコン等のエンドポイント端末から収集されるログ等のテレメトリデータをクラウド上に集約し、リアルタイムで相関分析を行う仕組みを実装[22]した。この仕組みにより、高度標的型攻撃を含む攻撃の兆候を即時に検出する機能を実現し、提供を開始した。2015 年に IBM は、自社の脅威インテリジェンス情報の分析集団である IBM X-Force が収集した、IoC や脆弱性情報、攻撃キャンペーン情報等をクラウドで公開した。これにより、ユーザはクラウドを介して脅威インテリジェンス情報を検索・共有[23]できるようになった。

2020 年代は、脅威インテリジェンス提供サービスと SIEM や SOAR 等の他セキュリティ製品の連携が進むとともに、AI を活用した脅威インテリジェンス情報のスコアリングや優先順位付けの高度化が加速した。例えば 2020 年に Palo Alto Networks は、脅威インテリジェンス情報を提供するプラットフォーム AutoFocus と SOAR 製品 Cortex XSOAR を統合し、IoC 等の脅威インテリジェンス情報の分析を基にした封じ込め等のインシデン

[21] U.S. Securities and Exchange Commission (https://www.sec.gov/Archives/edgar/data/1053148/000119312506178272/dex991.htm)
[22] U.S. Securities and Exchange Commission (https://www.sec.gov/Archives/edgar/data/1535527/000104746919003508/a2238988zs-1a.htm)
[23] PR Newswire (https://www.prnewswire.com/news-releases/ibm-opens-threat-intelligence-to-combat-cyber-attacks-300066816.html)

ト対応の自動化を実現[24]した。2025 年に Anomali は、AI を活用し、オープンソース情報(OSINT)や、SIEM・EDR 等の自社セキュリティ製品から得られるテレメトリを統合的に分析し、組織にとって重要度の高い脅威インテリジェンス情報を自動的に識別・優先順位付けする機能の提供を開始[25]した。

表 2-3-6　2000 年代から 2020 年代までの脅威インテリジェンス提供サービスの変遷

	2000年代	2010年代	2020年代
主要企業	脅威インテリジェンスサービス立ち上がり	ビッグデータ活用による分析高度化	他製品との連携／AIの活用
CrowdStrike（米国）		**CrowdStrike Falcon** • 2013年、エンドポイントからのテレメトリを収集し、クラウド上で相関分析し、IoC等の脅威情報を提供。 • また「Falcon Intelligence」等の脅威レポートの提供を開始し、高度持続的脅威（APT）の早期検出・対応を支援。	**CrowdStrike Falcon** • 2020年、AWSの「AWS Network Firewall」との統合を発表し、CrowdStrike Falconプラットフォームから配信されるIoCを基に、ネットワーク層の防御強化を支援。
IBM（米国）	**ISS X-Force** • 2006年頃IBMはISSを買収し、ネットワーク・エンドポイント・インシデント情報や脆弱性情報を収集し、API（JSON形式）で提供。日々の攻撃動向レポートも発行。	**IBM X-Force Threat Intelligence** • 2015年、IBM X-Forceチームが累積した脅威情報（Webページ25B件以上、270Mエンドポイントのマルウェア情報、12M件/日以上のスパム等）をクラウド化し、ユーザー間での共有や検索、ビッグデータを活用した相関分析を実現。	**IBM X-Force Threat Intelligence** • IBMはWatson AIおよび独自の機械学習モデルを活用して、1500億件／日超のセキュリティイベントから迅速に脅威発見・早期警告を行う機能を強化し、2024年には、QRadar Suite（SIEM製品）等との自動連携を発表。
Check Point Software Technologies（イスラエル）		**ThreatCloud** • 2012年、世界各地のセンサやゲートウェイから収集したテレメトリデータを基に、IoCを各製品へ配信する仕組みの提供を開始。	**ThreatCloud AI** • 2025年、50以上のAIモデルを活用した大規模なテレメトリーデータの収集・分析を実現し、未知の脅威に対する検出精度を強化。
Cisco Systems（米国）	**IntelliShield** • 2005年頃、世界中のデバイスセンサーからのテレメトリを集約し、脆弱性やマルウェアの侵入経路や、DDoSやキャンペーン発生状況等の情報を提供。	**Cisco Talos** • 2014年、CiscoがSourcefireのVulnerability Research Teamを買収し、脅威インテリジェンスの提供を加速。 • 世界中のネットワーク・エンドポイント・オープンソース等から脅威情報を収集し、IoCやTTPをリアルタイムで分析。	**Cisco Talos** • Ciscoは、Cisco Talosの脅威情報をSplunk ES/Attack Analyzerに取り込み、相関分析を自動化することを発表し、今後、Splunk Enterprise Security、Splunk SOARでも統合が予定されている。
Fortinet（米国）	**FortiGuard Labs** • 2002年頃、世界中のデバイスセンサーから、AV・IPS・Web URL・Antispam・脆弱性等の多層データを収集し、シグネチャやレピュテーションフィードを提供。	**FortiGuard Threat Intelligence Service** • 2017年頃、FortiGuard Labsが収集したIoC（悪性IP、ドメイン、URL、マルウェアハッシュ等）をクラウド経由で各種自社製品に配信を開始。	**FortiGuard AI** • 2018年頃、テレメトリデータを基に、AIがIoCや脆弱性情報をリアルタイムで分析する「FortiGuard AI」の提供を開始。
Anomali（米国）		**Anomali ThreatStream** • 2013年、Anomaliは異なるログソースやTIフィードを統合するTIP（Threat Intelligence Platform）を提供。 • 2016年には顧客自身が収集したログをSaaS上へアップロードしてリアルタイム照合するビッグデータ処理機能を追加。	**ThreatStream AI Professional Enterprise** • 2025年、外部の脅威フィードと自社環境のSIEM／EDRログをMLで相関付けし、「自社環境に影響を及ぼしうる脅威」をスコアリングし、ダッシュボード上でリアルタイムに可視化する製品を提供。

7．　MDR に関する製品の一覧及びその年代ごとの推移

表 2-3-7 に、2010 年代から 2020 年代までの MDR の変遷を示す。

2010 年代は、セキュリティツールの運用や脅威の監視を担うマネージドセキュリティサービスが、脅威への対応までを含むサービスへと拡張されたことにより、MDR としてセキュリティ市場で広く認知され始め、各社がサービス強化を進めた年である。例えば、Accenture は 24 時間対応のグローバル監視、分析、応答を行うマネージドセキュリティサービスを導入し、MDR の基盤を構築[26]した。Arctic Wolf Networks は、AWN CyberSOC を発表し、脅威の早期検知と迅速なインシデント対応を行う MDR を提供開始し、その後サービスの名称を Arctic Wolf Managed Detection and Response に変更[27]した。CrowdStrike は、Falcon プラットフォームを活用した脅威の検知と大規模な情報漏えいを防止するセキュリティサービスである Falcon OverWatch を提供開始し、その後 Falcon OverWatch を含む複数のサービスを組み合わせた MDR[28]である Falcon Complete を発表した。

[24] Palo Alto Networks(https://www.paloaltonetworks.jp/company/press/2020/palo-alto-networks-introduces-cortex-xsoar--redefines-security-orchestration-and-automation-with-integrated-threat-intel-management)
[25] Anomali(https://www.anomali.com/press/anomali-introduces-new-threatstream-for-the-age-of-ai)
[26] Accenture(https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/Accenture-CSS-MSS-Service-Description.pdf)
[27] Arctic Wolf Networks(https://cybersecurity.arcticwolf.com/rs/840-OSQ-661/images/AW_Managed_Detection_Response_Datasheet.pdf)
[28] CrowdStrike(https://www.crowdstrike.jp/wp-content/uploads/2021/05/Falcon-Complete-Datasheet_JA_202105.pdf)

2020 年代は AI を活用することにより、脅威への対処優先順位を自動で付けることが可能となり、セキュリティアナリストは注力すべきアラートに集中できることが可能となった。Accenture は Google の脅威インテリジェンス提供サービスや運用プラットフォーム、AI と連携[29]させ、自社の MDR の強化を図った。Tata Consultancy Services は、AI や機械学習を活用した 24 時間 365 日の脅威の監視、インシデント対応、修復を行う MDR の提供を開始[30]した。CrowdStrike は、AI を活用した MDR である CrowdStrike Falcon Complete Next-Gen MDR を提供[31]し、脅威への対処の効率化を図った。このように、MDR は他社との連携や AI や機械学習を活用することで、サービスの高度化及び効率化を進めている。

表 2-3-7　2010 年代から 2020 年代までの MDR の変遷

	2000年代	2010年代	2020年代
主要企業		MDRの登場	AIの活用・他社との連携拡大によるサービス強化
Accenture（アイルランド）		**Managed Security Services** • Accentureは24時間365日のリアルタイム監視、分析、報告を行うセキュリティサービスを提供。	**Managed Extended Detection and Response** • 2023年に、Googleと連携強化を図り、Googleの脅威インテリジェンスやプラットフォーム、AIを活用することにより、セキュリティサービスを強化。 • 2025年に、政府向けのセキュリティサービスであるMxDR for government solutionを提供開始。
Arctic Wolf Networks（米国）		**AWN CyberSOC** • Arctic Wolf Networksは中堅企業を対象とした、脅威の早期検知と迅速なインシデント対応を行うセキュリティサービスを提供。 • 2010年代後半に、AWN CyberSOCの名称をArctic Wolf Managed Detection and Responseと変更。	**Arctic Wolf Managed Detection and Response** • 2025年に、Arctic Wolf NetworksのMDRを支えるプラットフォームであるAurora Platformに、アラートの要約やインシデントの分析等を行うAIを導入。
CrowdStrike（米国）		**CrowdStrike Falcon OverWatch** • CrowdStrike Falconプラットフォームを活用し、脅威の検知と情報漏洩防止を支援するセキュリティサービスを提供。 • 2018年に、導入、保守から対応、修復までを行うCrowdStrike Falcon Endpoint Protection Completeを提供開始。	**CrowdStrike Falcon Complete Next-Gen MDR** • 2024年に、AIを活用することにより脅威の早期遮断実現を目的としたCrowdStrike Falcon Complete Next-Gen MDRを提供開始。
Deloitte Touche Tohmatsu（英国）		**Managed Security Services** • クラウドやアプリケーション、IoT、産業用制御システム等の幅広い対象に対応可能なセキュリティサービスを提供。	**Managed Extended Detection&Response by Deloitte** • 2022年に、Deloitteは脅威の検知や対応、修復を行うセキュリティサービスを提供開始。 • 2025年に、Palo Alto NetworksのCortex XSIAMプラットフォームを統合。
NTTデータ（日本）		**Managed Security Services** • サービスの導入や脅威の検知、インシデント調査に強みを持つセキュリティサービスを提供。	**MDRの提供開始** • 2023年に、NTTデータは日本国内に向けて脅威の未然防止から脅威への対処、再発防止までを行うセキュリティサービスを提供開始。
Tata Consultancy Services（インド）		**Cyber Security Managed Services** • セキュリティオペレーションセンタによる脅威インテリジェンスの共有や脅威の監視・対応を行うセキュリティサービスを提供。	**TCS'Managed Detection and Response services** • AIを活用した24時間365日の脅威の監視、対応、修復を行うセキュリティサービスを提供。 • 2024年に、CrowdStrikeと連携し、AIを基盤としたCrowdStrike Falcon XDRプラットフォームを導入。

8．　Firewall 製品に関する製品の一覧及びその年代ごとの推移

表 2-3-8 に、2000 年代から 2020 年代までの Firewall の変遷を示す。

2000 年代は、UTM や次世代 Firewall が台頭した年であり、例えば 2002 年 Fortinet が UTM である FortiGate を市場へ投入[32]し UTM の先駆けとなり、Juniper は従来型の Firewall に IPS を統合した製品 SRX シリーズの提供を開始[33]した。その他 Cisco Systems は ASA5500

[29] Accenture（https://newsroom.accenture.jp/jp/news/2023/release-20230524）
[30] Tata Consultancy Services（https://www.tcs.com/what-we-do/services/cybersecurity/solution/managed-detection-response-services）
[31] CrowdStrike（https://www.crowdstrike.com/en-us/press-releases/crowdstrike-falcon-complete-next-gen-mdr-sets-the-new-standard-for-managed-detection-and-response/）
[32] Fortinet（https://investor.fortinet.com/news-releases/news-release-details/fortinet-celebrates-10-years-innovation-and-leadership-security）
[33] Juniper Networks（https://d1lge852tjjqow.cloudfront.net/CIK-0001043604/1c5eec2a-de7f-4f1b-984e-328e070e6eae.pdf）

シリーズ[34]、Palo Alto Networks は PA-4000[35]シリーズの提供を開始し、従来のネットワーク層の制御に加え、不正侵入検知(IDS)や不正侵入防御(IPS)機能や、アプリケーション層での制御機能の追加等の多機能化が促進した。

2010 年代は、仮想型 Firewall が台頭した年であり、例えば Palo Alto Networks はオンプレミス、ハイブリッドクラウド、クラウド環境のいずれにも対応した VM シリーズの提供を開始[36]し、Barracuda は物理アプライアンス同等のセキュリティ機能を有し、仮想マシン用に最適化された Barracuda CloudGen Firewall Virtual の提供を開始[37]した。また、Check Point Software Technologies は、Check Point vSEC Virtual Edition の提供を開始[38]する等、クラウド化の促進を背景に、仮想アプライアンスの提供が拡大した。

2020 年代は、AI による Firewall の設定・運用の自動化が加速した年であり、例えば 2020 年に Palo Alto Networks によって、不審ファイルやフィッシング攻撃を検知・ブロックできるよう AI を搭載した次世代 Firewall の提供が開始[39]された。2023 年に Cisco Systems は、Secure Firewall の製品群に対して Cisco AI Assistant for Security を統合することで、重複するポリシの検出と最適化提案の自動化等を実現し、Firewall の効率的なポリシ管理を AI によって強化[40]した。また、クラウド化促進に伴い、従来の境界防御型モデルから、ユーザやデバイスの認証・アクセス制御を常時検証するゼロトラストの仕組みを備えた製品の提供が開始された。Firewall 製品は、2000 年代から現在の 2020 年代にかけて物理的な単一ボックスから AI を搭載したクラウド型防御へと変化している。

[34] Cisco Systems (https://www.cisco.com/web/UK/news/pdfs/2005/03_05_2005_asa_final_release.pdf)
[35] Palo Alto Networks (https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdf)
[36] Palo Alto Networks(https://www.paloaltonetworks.com/blog/2012/11/the-biggest-product-launch-in-the-history-of-palo-alto-networks/)
[37] Barracuda Networks(https://www.prnewswire.com/news-releases/barracuda-announces-new-cloud-generation-firewall-capabilities-300556381.html)
[38] Check Point Software Technologies(https://www.checkpoint.com/press-releases/check-point-vmware-software-defined-data-center-advanced-security/)
[39] Palo Alto Networks(https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-launches-worlds-first-ml-powered-ngfw)
[40] Cisco Systems(https://blogs.cisco.com/developer/cisco-ai-assistant-for-managing-firewall-policies-is-now-available)

表 2-3-8　2000 年代から 2020 年代までの Firewall の変遷

	2000年代	2010年代	2020年代
主要企業	UTMや次世代Firewallの台頭	仮想アプライアンスの台頭	機能高度化とAIによる自動化
Palo Alto Networks（米国）	PA-4000シリーズ • Palo Alto Networksが2007年にポート依存を排し、暗号化通信でもアプリケーションを識別する最初のNGFWの提供を開始。	VM-シリーズ • 2012年、Palo Altoはオンプレミス、ハイブリッドクラウド、クラウド環境のいずれにも対応したVM-Seriesをリリースし、パブリッククラウド上でのNGFWの提供を開始。	PAN-OS 10.0 • 2020年、Palo Altoは世界初のML（機械学習）搭載NGFW、インラインで不審ファイルやフィッシング攻撃を検知・ブロック、ポリシを自動推奨することで未知脅威への即時対処を実現できるPAN-OS 10.0をリリース。
Cisco Systems（米国）	ASA 5500シリーズ • Ciscoは2005年にPIX後継としてASA 5500シリーズを市場へ投入し、2010年にはIPAIエンジンを強化したASA 5500-Xを発表し、IPSやVPN性能を大幅に向上。	ASA 1000V Cloud Firewall • 2012年、物理的なFirewallと同様の機能を提供するVMware環境向けの仮想的Firewallの提供を開始。	Cisco Secure Firewall • 2024年頃、CiscoはSecure Firewall製品群に「Cisco AI Assistant for Security」を統合し、ポリシー管理の自動化や、トラブルシューティング支援をAIにより強化。
Fortinet（米国）	FortiGate • 2002年にFortinetが初代FortiGateを市場投入し、「UTM」という概念を牽引し、ASICベースで数Gbpsを実現。	FortiGate-VM • VMware等の仮想化基盤に対応した、物理的Firewallと同じOS（FortiOS）で稼働する仮想型Firewallの提供を開始。	Fortinet FortiGuard AI-Powered Security Services • 2025年、Workspace Security Suiteを発表し、FortiGuardが提供するAIベースの脅威インテリジェンスをリアルタイムに適用し、機械学習による振る舞い検知で未知マルウェアの自動ブロック機能を追加。
Juniper Networks（米国）	SRXシリーズ • Juniperは2009年末にSRXシリーズを発表し、従来型Firewall＋IPSを統合した最初期のアプライアンスの提供を開始。	V-SRXシリーズ • 2014年、VMwareなどの環境で動作する仮想Firewallの提供を開始し、その後AWSやAzure等のクラウド対応も拡充。	SRXシリーズ • 2021年、Mist AIプラットフォームとFirewallのSRXシリーズを連携させることで、Firewallの初期設定をAIにより自動化する機能を発表。
Huawei Technologies（中国）	Unified Security Gateway • 2003年、ネットワーク・プロセッサアーキテクチャに基づき、初のFirewallの提供を開始	Huawei USG Virtual Firewall • 2015年、物理的FirewallであるUnified Security Gateway「USG」と同様の機能を、VMwareやKVMなどの仮想環境上で実現するFirewallの提供を開始。	HiSecEngine USG12000シリーズ • 2018年にサービス構成や要件に応じたセキュリティポリシーの設定をAIによって自動化し、その設定を他Firewallへ配布できる仕組みを提供。
Check Point Software Technologies（イスラエル）	UTM-1 • 2007年、中小企業向けにUTM（統合脅威管理）デバイスとしてアンチウイルス、IPS、URLフィルタリングなど機能を単一の製品として統合した製品の提供を開始。	Check Point vSEC Virtual Edition • 2015年、物理アプライアンスと同等のFirewall、VPN、IPS、アンチウイルス等を有し、VMware、Hyper-V、KVM対応の仮想セキュリティゲートウェイの提供を開始。	Check Point CloudGuard Network Security • 現在、イスラエルのセキュリティ企業TufinがTufin Orchestration Suiteと自社Firewall製品を連携させることで、AIを活用したセキュリティルールの自動設定を提供。

9．　Sandbox 製品に関する製品の一覧及びその年代ごとの推移

表 2-3-9 に、2000 年代から 2020 年代にかけての Sandbox の変遷を示す。2000 年代はマルウェアの感染経路の多様化、2010 年代はクラウド環境の普及、2020 年代は AI や機械学習の機能向上といった時代ごとの特徴に応じて、Sandbox 製品はその在り方を変化させてきた。

2000 年代は、Sandbox 製品が登場した時期である。完全にエミュレートされた Windows 環境でコードを実行し、マルウェアの挙動を分析する Norman Sandbox[41]は、その代表例であり、Norman ASA によって提供された。

2010 年代に入ると、クラウド環境の普及に伴い、Sandbox 製品はクラウド環境への対応を進めた。例えば、Cisco Systems はマルウェアをクラウド上で収集し、動的分析や静的分析により、マルウェアを分析する Cisco Advanced Malware Protection Threat Grid を提供[42]した。Check Point Software Technologies は SandBlast Cloud を通じて、クラウド環境でやり取りされる電子メール向けの Sandbox 製品である SandBlast Cloud を提供[43]した。Fortinet は NGFW 等のセキュリティ製品と統合可能な FortiSandbox-3000D[44]を提供することで、高度な脅威検出と拡張性を実現した。また、Symantec はクラウド環境でのセキュリティ事業を強化するために、Norman ASA を分割した企業である Norman

[41] PR Newswire(https://www.prnewswire.com/news-releases/norman-sandbox-anti-malware-security-technology-recognized-as-most-innovative-idea-in-past-decade-at-vb2010-conference-104484214.html)
[42] Cisco Systems(https://www.cisco.com/c/ja_jp/products/collateral/security/amp-threat-grid-cloud/datasheet-c78-733495.html)
[43] Check Point Software Technologies(https://blog.checkpoint.com/security/introducing-check-point-sandblast-cloud/)
[44] Fortinet(https://investor.fortinet.com/news-releases/news-release-details/fortinetr-introduces-new-advanced-threat-detection-mitigation)

Shark を傘下に加えた BlueCoat を買収[45]した。

2020 年代には、AI と機械学習の活用が進み、Sandbox 製品は判定の高速化を実現している。例えば、Trellix は動的解析、静的解析、機械学習を活用した Intelligent Sandbox を提供[46]している。Fortinet の FortiSandbox5.0[47]は、AI エンジンを活用した Sandbox 製品であり、判定時間を従来の 10 分の 1 に短縮している。さらに検知精度を従来の 3 倍向上させており、未知の脅威に対してリアルタイムで防御を可能としている。Palo Alto Networks の Advanced WildFire[48]は、機械学習に基づく検出エンジンを使用しており、マルウェアのシグネチャ生成の高速化を図っている。このように、Sandbox 製品は専用型からクラウド型へと移行し、AI や機械学習の発展に伴い、より迅速かつ精度の高い脅威検知を実現している。

表 2-3-9　2000 年代から 2020 年代までの Sandbox の変遷

	2000年代	2010年代	2020年代
主要企業	Sandbox製品の登場	クラウド環境への対応	AI・機械学習の活用による判定の高速化
Broadcom（米国）	**Norman SandBox** • Norman ASAは、Windows環境を模倣した環境でマルウェアを自動的に分析することが可能なSandbox製品を提供。	**Symantecによるクラウド環境でのセキュリティの強化** • Norman ASAを分割した侵入防御ソリューションを提供するNorman SharkをBlueCoatが買収。 • 2016年にSymantecは、クラウド環境でのセキュリティ事業を強化するためにBlueCoatを買収。	**Symantec Cloud Sandbox** • Symantecのエンタープライズセキュリティ事業を買収したBroadcomは、機械学習を活用したSandbox製品であるSymantec Cloud Sandboxを提供。
Cisco systems（米国）		**Cisco Advanced Malware Protection Threat Grid** • マルウェアをクラウド上で収集し、動的分析や静的分析により、マルウェアを分析する。	**Cisco Secure Malware Analytics** • 数百万のファイルを解析し、解析済みのマルウェアのアーティファクトと相関付けることにより、マルウェア攻撃や攻撃キャンペーンを把握。
Check Point Software Technologies（イスラエル）		**SandBlast Cloud** • 2016年に、Check Point Softwareはクラウド環境でやり取りされる電子メール向けのSandbox製品であるSandBlast Cloudを発表。	**SandBlast** • 脅威インテリジェンスであるThreatCloud AIや、AI技術により未知の脅威からユーザを保護。
Fortinet（米国）		**FortiSandbox-3000D** • 2013年に、FortinetのNGFW等と統合可能なSandbox製品であるFortiSandbox-3000Dを発表。	**FortiSandbox 5.0** • AIエンジンが搭載されたSandbox製品であり、未知の脅威に対してリアルタイムで防御を行う。
Trellix（米国）		**FireEye Email Threat Prevention** • FireEyeは、メールを利用した標的型サイバー攻撃からネットワークを保護するために動的解析でマルウェアを分析するエンジンを使用したクラウド型サービスを提供。	**Trellix Intelligent Sandbox** • Trellixは、動的解析、静的解析、機械学習を活用したSandbox製品であるTrellix Intelligent Sandboxを提供。
Palo Alto Networks（米国）		**WildFire** • Palo Alto NetworksはクラウドベースのSandbox製品であるWildFireを提供。	**Advanced WildFire** • Palo Alto Networksは機械学習に基づく検出エンジンを使用したSandbox製品であるAdvanced WildFireを提供。

[45] Gem Digital(https://newsroom.gendigital.com/Symantec-to-Acquire-Blue-Coat-and-Define-the-Future-of-Cybersecurity)
[46] Trellix(https://www.trellix.com/assets/data-sheets/trellix-intelligent-sandbox-datasheet.pdf)
[47] Fortinet(https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf)
[48] Palo Alto Networks(https://www.paloaltonetworks.jp/network-security/advanced-wildfire)

要約

第３章　政策動向調査

第３章では、本テーマに関する政策の動向について取りまとめている。

第３章の要約

- サイバーセキュリティ戦略はサイバーセキュリティ基本法第 12 条に基づく国家戦略で、施策の方向性として「深刻化するサイバー脅威に対する防御・抑止」「幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上」「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」の３つを掲げている。
- サイバーセキュリティ対策本部第 43 回会合では、サイバーセキュリティ戦略に基づく府省庁別の予算・施策を整理している。
- 国家安全保障戦略はサイバー分野を主要領域の１つとしている。また、国家安全保障戦略では能動的サイバー防御の導入に向けた取組も示している。
- 日本のサイバー攻撃検知分野の助成施策は、内閣府や経済産業省等が中心となり、国家安全保障や次世代 ICT・通信技術の安全性向上を目的に幅広く展開されている。
- 日本国内におけるサイバー攻撃検知に関する技術の標準化・規格化の取組は、経済産業省と総務省が中心となって推進している。両省は国際的な標準化動向を踏まえ、協力機関と連携し、ガイドライン策定や啓発活動を進めている。
- 日本国内のサイバーセキュリティに関する倫理規制として個人情報保護法や電気通信事業法、サイバーセキュリティ基本法、サイバー対処能力強化法及び同整備法が挙げられる。
- 米国は 2023 年に国家サイバーセキュリティ戦略を策定し、予算規模は総額 175 億米ドルとなっている。また、本戦略では、サイバー攻撃の検知・防御を含む政策領域を５つの柱として整理している。
- 米国では、検知や分析時のプライバシー保護に適用され得る規制として Health Insurance Portability and Accountability Act 等が挙げられる。また、サイバー攻撃に対する国家や公共基盤の安全確保に適用される可能性のある規則として Federal Information Security Modernization Act 等が挙げられる。
- 欧州では、検知や分析時のプライバシー保護に適用され得る規制として EU General Data Protection Regulation(Regulation 2016/679)等が挙げられる。また、サイバー攻撃に対する国家や公共基盤の安全確保に適用される可能性のある規則として NIS Directive(Directive 2016/1148)等が挙げられる。
- 国際標準化団体は委員会やワーキンググループを通じ、検知技術の標準化を推進している。代表的な国際標準化団体として ISO や IEC、ITU 等が挙げられ、それぞれ団体が互いに協力を行いながら、標準化を進めている。
- 日本の標準化活動は国際的な規格との整合性を保ちつつ、国内の産業や社会のニーズに応じた規格の策定と普及を目的として進められている。標準化を推進する主要な団体である JISC や、各官公庁の管轄下にある関連団体が、標準化活動を推進している。
- 米国は国際規格を踏まえた規格の策定と、政府機関で実運用されるサイバーセキュリティフレームワークの策定及び公開を進めている。米国内で標準化を推進する主な団体としては ANSI や NIST、MITRE が挙げられる。

第１節　サイバー攻撃検知に関する政策動向

１．　サイバーセキュリティ戦略の概要[49]

サイバーセキュリティ戦略(2025 年 12 月閣議決定)は、サイバーセキュリティ基本法第 12 条に基づく国会報告として位置付けられ、今後 5 カ年の諸施策の目標と実施方針を示す国家戦略文書である。基本法制定後 4 回目の戦略となる本戦略は、国家安全保障戦略(2022 年 12 月国家安全保障会議決定及び閣議決定)との整合性を保ちつつ、厳しさを増す国際情勢や国家を背景としたサイバー脅威の増大、また、社会全体のデジタル化の進展に伴うリスクの顕在化に対応するものである。

本戦略では、顕在化するリスクを広く認識しており、近年ではより巧妙化、複雑化しデジタルと結びついた攻撃形態が増大していることを背景に、これらのサイバー脅威が業務停止、サービス障害、金銭被害、機密情報の窃取等により経済社会活動、ひいては国家安全保障に大きな影響を及ぼし得ることを課題認識としている。これらの課題に対し、「自由、公正かつ安全なサイバー空間」の確保を基本理念とし、「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」という 5 つの原則に基づき、国がこれまで以上に積極的な役割を果たすことを表明している。施策の方向性として、「深刻化するサイバー脅威に対する防御・抑止」「幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上」「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」の 3 つを掲げている。

（１）　深刻化するサイバー脅威に対する防御・抑止

2025 年 7 月に設置された国家サイバー統括室の司令塔機能を中核とし、重要電子計算機に対する不正な行為による被害の防止に関する法律(令和 7 年法律第 42 号、本報告書では「サイバー対処能力強化法」と呼ぶ。)に基づく通信情報の利用を含む情報収集・分析の強化を図る。特に能動的サイバー防御の導入は、本戦略における中核的施策の一つとして位置付けられており、アクセス・無害化措置を中核とし、警察と防衛省・自衛隊が共同対処する体制が構築される。また、2026 年秋からの新たな官民連携協議会には基幹インフラ事業者等が参加し、双方向・能動的な情報共有と対策のサイクルが確立される。国際面では、同盟国・同志国等との情報・運用面での協力強化、パブリック・アトリビューション等の実施、インド太平洋地域における能力構築支援、国際的なルール形成への積極的参画を推進する。

（２）　幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

政府機関等や重要インフラ事業者等は、国家を背景とした組織化・洗練化されたサイバー攻撃の標的となっている。被害を受ければ、国民生活や社会経済、ひいては国家安全保障に甚大な影響を及ぼすおそれがあり、これらの組織は自らの社会的責務を果たすためにサイバーセキュリティを確保する責任を負う。具体的には、政府統一基準群やISMAP の継続的な見直し、監視の結果等を活用したメリハリのある監査、デジタル庁との連携によるセキュリティ・バイ・デザインの推進が実施される。2026 年度には重要イ

[49] サイバーセキュリティ戦略本部 サイバーセキュリティ戦略(2025 年 12 月 23 日閣議決定)
(https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf)

ンフラ統一基準を新規策定し、サイバー対処能力強化法に基づく基幹インフラ事業者の届出・インシデント報告等の枠組みを整備する。さらに、自らが遂行すべき業務や製品・サービスからエンドユーザに至るサプライチェーン全体の信頼性確保に努める「任務保証」の考え方の下で、サイバーセキュリティを確保し、レジリエンスを高めていく。ベンダや中小企業等のリスクに応じた対策水準の可視化・確認制度の整備、個人・中小企業への支援策の拡充、サイバー犯罪対策(国際共同捜査、フィッシング・詐欺対策、国民のリテラシー向上)も推進される。

（3） 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

我が国は、デジタル技術・産業そのものも相当程度海外に依存しており、サイバーセキュリティ分野も同様である。安全保障の観点からも、我が国に基盤を持つ形での国内産業の育成や、技術力・開発力の向上等を通じた自律性の確保が求められる。サイバーセキュリティ分野における対応能力を向上させるためにも、海外の技術やサービスに過度に依存することなく、国内において新たな技術及びサービスの研究開発、実証等を活性化させる必要がある。早期の社会実装により分析力・開発力を向上させる等、国産技術・サービスを核とした、技術、人材を育成する好循環のエコシステムを形成していく。人材面では、サイバーセキュリティ人材の定義の明確化、スキルに応じた研修・演習の体系化、官民人材交流の促進、外部専門人材の登用拡大を進める。技術面では、AI を活用したサイバーセキュリティ確保(AI for Security)に関して、膨大なデータの処理や高度な分析が求められる中、政府は関係主体と連携しつつ AI を活用したサイバー攻撃インフラの検知や関連情報の分析の精緻化・迅速化等を推進する。また、政府機関は 2035 年までに耐量子計算機暗号(PQC)への移行を目標とする。

2． 各省庁でのサイバーセキュリティ施策

サイバーセキュリティ対策本部第 43 回会合(2024 年 5 月)では、サイバーセキュリティ戦略に基づく府省庁別の予算・施策が整理されている[50]。2025 年度当初予算におけるサイバーセキュリティ関連予算は約 2,051 億円であり、その分野別内訳は、経済社会の活力向上と持続的発展、国民が安全で安心して暮らせるデジタル社会の実現、国際社会の平和・安定及び我が国の安全保障への寄与、横断的施策として示されている。

以下では、2025 年度の政府の主なサイバーセキュリティ施策のうちサイバー攻撃検知に関連する内容と当初予算額を述べる。

[50] サイバーセキュリティ戦略本部　政府のサイバーセキュリティに関する予算(第 43 回戦略本部会合 資料 6)(https://www.cyber.go.jp/pdf/council/cs/dai43/43shiryou6.pdf)

表 3-1-1　各省庁におけるサイバー攻撃検知に関するサイバーセキュリティ施策

所管省庁	主な施策	概要	2025 年度当初予算額（億円）
内閣官房	政府機関情報セキュリティ横断監視・即応調整チームの運用	政府関係機関情報セキュリティ横断監視・即応チーム(GSOC)は、NISC の下で政府機関等のネットワークや情報システムを 24 時間 365 日体制で横断監視し、不正な通信の検知、マルウェア解析、脅威情報や脆弱性情報の提供等を通じて各府省庁のインシデント対応を支援する枠組みである。2024 年度からは、政府機関等の情報システムをインターネット上から常時評価し、脆弱性等の随時是正を促す「横断的アタックサーフェスマネジメント(ASM)」と、悪意ある Web サイトやマルウェア等へのアクセスを DNS レベルで遮断しつつ関連するドメイン名・IP アドレスを検知・収集する「プロテクティブ DNS(PDNS)」を導入し、常時診断・対応型のセキュリティアーキテクチャを実装している。2025 年度年次計画では、巧妙化・高度化する攻撃に対応するため、GSOC システムの要素技術の実証と改善を進めること、ASM との一体的運用により脆弱性対応を一層効果的にすること、PDNS の導入を図ることで関係主体全体のセキュリティレベルを底上げし、GSOC 監視等のオペレーションを強化することが示されている。	16.0
内閣官房	政府機関等に対するサイバーセキュリティの実践的検証	国家安全保障戦略が掲げる「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」との方針に基づき、国家サイバー統括室の対応能力を高めるための取組である。Living Off The Land(LOTL)攻撃(システム内寄生攻撃)等、高度なサイバー攻撃の検知能力を向上させ、国家安全保障上重要な政府機関等へのセキュリティ対策を重点化	5.0

所管省庁	主な施策	概要	2025 年度当初予算額（億円）
		するとともに、検知ノウハウを広く共有することを狙いとしている。具体的には、仮想環境上で疑似攻撃を実行し、検知手法・ルールを検証・評価・改善する取組に加え、実際の政府機関等を対象として、リスクシナリオに基づくリスク評価、検知手法・ルールを適用した侵入試験、検知ログ分析ツールを用いた脅威探索を実施し、その結果から検知手法・ルール及びツールを精緻化する。また、これらの実践的検証を担う職員を計画的に育成し、政府機関等における実践的検証を恒常的に実施できる体制を整備することで、政府全体のサイバーセキュリティ対応能力の抜本的な強化につなげることを目指す。	
総務省	IoT の安心・安全かつ適正な利用環境の構築	本施策は、急増する IoT 機器がボットネット化し、DDoS 攻撃の踏み台となることを防ぐことを目的としている。総務省と NICT は NOTICE(National Operation Towards IoT Clean Environment)を通じ、初期パスワードのまま利用される機器や推測容易な ID・パスワードを用いる機器、マルウェア感染により不審な通信を行う機器を継続的に調査し、ISP 事業者経由で利用者に注意喚起する。さらに、NICTER 等で観測したトラフィックを解析し、ボットネットの C&C サーバや攻撃元インフラを検知・把握することで、大規模 DDoS 攻撃の予兆把握と迅速な封じ込めを図る。これらの結果を、利用者の設定改善や事業者による遮断措置、機器メーカーのファームウェア改修等につなげるとともに、関係省庁や業界団体と連携したルール整備・周知啓発を進めることで、家庭用機器から産業用制御シ	15.8

所管省庁	主な施策	概要	2025 年度当初予算額(億円)
		ステム、スマートホーム・スマートシティまで、IoT エコシステム全体のセキュリティ水準の底上げを目指す。	
総務省	政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業	政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業(CYXROSS)は、海外製のセキュリティ製品への依存を低減し、国産技術を核とした自律的な対処能力を構築することを目的とする。総務省と NICT は、安全性・透明性の検証が可能なソフトウェアセンサーを開発し、サイバーセキュリティ対策の優先度が高い府省庁の端末に導入することで、マルウェア感染端末の振る舞いやアラート、検体情報等の実データを数千台規模で収集し、CYNEX(NICT が所管する産学官連携基盤)上に集約して分析する。この分析により、攻撃傾向や IoC といった国産の脅威情報を生成し、政府機関へフィードバックすることで、政府システムの検知・防御能力の高度化と、我が国独自のサイバー情勢分析能力の強化を図るとともに、将来的な国産セキュリティ製品・サービスの創出につなげる狙いがある。	13.0
警察庁	生成 AI を活用したフィッシングサイト判定の高度化・効率化	警察庁では急増するフィッシング詐欺から利用者を保護するため、フィッシングサイトの URL や画面構成、文章表現等の特徴量を生成 AI で分析し、正規サイトとの類似性や不自然な点を自動判定することで、従来人手で行っていた判定作業の高度化・効率化に取り組む。また、「サイバーセキュリティ 2025」における安全・安心なデジタル利用環境の確保という方向性とも整合し、キャッシュレス決済やインターネットバンキングに対する攻撃に対し、警察・事業者双方の対	0.3

所管省庁	主な施策	概要	2025 年度当初予算額（億円）
		処能力を底上げし、利用者が意識せずとも被害に遭いにくい環境整備を図ることが期待されている施策である。	
国土交通省	航空管制セキュリティシステム	本システムは航空交通管制情報処理システムや関連ネットワークを対象に、サイバー攻撃から航空機の安全な運航を守るための国土交通省の情報システムである。エアラインや海外の管制機関等と飛行計画情報等をやり取りする性質上、外部ネットワークとの接続を前提としており近年の攻撃の巧妙化・高度化を踏まえると、従来型の境界防御のみではリスクが残存する。このため、2025 年度は、通信経路の多層防御、監視・ログ分析基盤の強化、異常時のフェイルセーフ確保等、システム全体の堅牢化に向けた具体的な対策要件を整理することが掲げられている。また、重要インフラ分野におけるランサムウェアや DDoS 攻撃が航空分野にも影響を与えた事例が示されていることも踏まえ、航空分野における事業継続計画や復旧手順との一体的な見直しを進めることで、サイバー攻撃時にも航空交通の安全とサービス継続を確保することを目指す。これらを通じて、空港や航空会社を含む関係主体のセキュリティ水準を底上げし、航空ネットワークの信頼性維持にも貢献することが期待されている。	11.6
防衛省	情報システムの防護	情報システムの防護は、防衛省が防衛力抜本的強化の一環として推進する、中核的なサイバーセキュリティ施策である。高度化・巧妙化するサイバー攻撃から、自衛隊の任務遂行を支える装備品や指揮統制システム、施設インフラを含む各種情報システムを防護し続けることを	876.3（※機材調達や運用費も含まれる）

所管省庁	主な施策	概要	2025 年度当初予算額（億円）
		目的としている。ゼロトラスト概念に基づくセキュリティ機能の導入指針を策定し、ユーザや端末、アプリケーションごとにきめ細かなアクセス制御や認証を行う体制の構築を進めるとともに、自衛隊の基幹システムを統合・共通化したクラウド基盤を整備し、一元的な監視・防護を可能とする。また、防衛省への攻撃手口や痕跡を収集・分析するサイバー防護分析装置等の整備を通じ、脆弱性管理やインシデント対応の高度化を図る。サイバーセキュリティ 2025 で示された安全保障の観点からの取組強化とも連動し、将来にわたり防衛情報資産の機密性・完全性・可用性を確保する体制の構築を目指す中核的な施策である。	

３．　サイバー安全保障戦略の概要

国家安全保障戦略(2021 年 12 月閣議決定)は日本の安全保障政策の最上位文書であり、サイバー分野を安全保障上の主要領域の一つとして位置付けている。この文書では、サイバー分野における対応として、同盟国・同志国との連携強化、攻撃の兆候把握・分析能力の向上、被害の最小化に向けた体制整備等を通じ、日本のサイバー安全保障上の能力を主要先進国と同程度の水準に引き上げる方針を掲げている。加えて、国家安全保障戦略では能動的サイバー防御の導入に向けた取組として 3 つの柱を示した。サイバー攻撃等に関する民間との情報共有・対処調整・支援等の強化、通信事業者の情報を活用した、攻撃者が悪用するサーバ等の検知、重大なサイバー攻撃前の攻撃者のサーバ等への侵入・無害化である。これらに基づいて 2024 年から能動的サイバー防御に関する有識者会議を立ち上げ、現状の課題や目指すべき方向性について議論しており、必要な法整備や組織体制の構築が推進されている。

第２節　各省庁の助成施策

日本におけるサイバー攻撃検知分野の助成施策は、内閣府・経済産業省・総務省・文部科学省・防衛省を中心に、国家安全保障や次世代 ICT・通信技術の安全性向上を目的として幅広く展開されている。また、研究開発や実証を推進する手法としては、各府省庁又は独立行政法人が研究開発・調査・実証等の業務を外部機関に契約により委託し、契約に基づく成果物の提出を求める仕組みが主流となっている。

表 3-2-1　国内のサイバー攻撃検知に関する助成施策一覧

担当省庁	施策	概要
内閣府 経済産業省 (NEDO)	経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化[51]	期間：2024 年 7 月～2029 年 6 月。 予算規模：総額最大 290 億円。 施策位置付け：経済安全保障重要技術育成プログラムのサイバー分野におけるプロジェクト。 目的：AI を活用した攻撃等のサイバー空間での顕在化したリスクへの対策として、サイバー空間の状況把握力と防御力の向上や環境整備を遂行。 開発研究項目：マルウェア機能の自動抽出等。
内閣府 (NEDO)	IoT 社会に対応したサイバー・フィジカル・セキュリティ[52]	期間：2018 年～2022 年。 予算規模：総額 107.57 億円。 施策位置付け：戦略的イノベーション創造プログラム(SIP)第 2 期における物理とサイバーの融合領域(CPS)領域のセキュリティ向上プロジェクト 目的：IoT デバイスの CPS におけるセキュリティの確保。研究開発項目：情報の発生源から利用先までの信頼を保証するデータ流通インフラの構築・運用監視・障害発生時の評価・復旧。 ※終了した施策のため、「サイバーセキュリティ 2025」に記載なし
総務省 (NICT)	Beyond 5G 研究開発推進事業	制定：2020 年。 サイバーセキュリティ以外も含めた予算規模：約 300 億円/年度。 目的：Beyond 5G(6G)に向け、通信インフラ、セキュリティ等において、世界をリードする革新的技術を日本主導で研究・実証すること。 研究課題例：2022 年度の「Beyond 5G 機能実現型プログラムのうち一般課題」で「デジタルツインによるサイバー・フィジカル連携型セキュリティ基盤」[53]が採択され、CPS 全体での自律的なセキュリティ確保技術を研究。
文部科学省 (JST)	戦略的創造研究推進事業(CREST・さきがけ・ACT-X)	制定：2020 年。 サイバーセキュリティ以外も含めた予算規模：約 500 億円/年度。 目的：国の科学技術基本計画に基づく基礎研究の推進。 研究課題例:「基礎理論とシステム基盤技術の融合

[51] NEDO(https://www.nedo.go.jp/news/press/AA5_101762.html)
[52] NEDO(https://www.nedo.go.jp/activities/ZZJP_100156.html)
[53] NICT(https://www.nict.go.jp/publicity/topics/2022/08/05-1.html)

担当省庁	施策	概要
		による Society5.0 のための基盤ソフトウェアの創出(2022 年 10 月～2028 年 3 月、総額最大 5 億円)」[54]では、Society 5.0 社会を支える『基盤ソフトウェア技術』の確立等を目的とし、AI 駆動型サイバーフィジカルシステムのセキュリティ評価・対策基盤の研究開発を実施。
防衛省 (防衛装備庁(ATLA))	安全保障技術研究推進制度	制定：2018 年。 サイバーセキュリティ以外も含めた予算規模：100 億円程度/年度。 目的：将来の防衛分野での活用に向け基礎研究の発掘・育成。研究課題例：2025 年度公募の 22 テーマの 1 つに「サイバーセキュリティに関する基礎研究」[55]が含まれ、AI 技術等による自動でサイバー攻撃に対処可能なシステムの実現等の課題解決・研究を募集。

第３節　国内の標準化・規格化に関する政策動向

日本国内におけるサイバー攻撃検知に関する技術の標準化・規格化の取組は、主に経済産業省と総務省が中心となって推進している。また、両省は国際的な標準化動向を踏まえ、IPA とも連携しつつ、ガイドラインの策定や啓発活動を進めている。国内の標準化・規格化に関する政策動向は表 3-3-1 に示している。

表 3-3-1　国内の標準化・規格化に関する政策動向一覧[56]

担当省庁	施策	概要
経済産業省	SSDF の実装および SBOM 活用促進の検討	米国では、NIST が策定したソフトウェアの脆弱性を軽減することを目的としてソフトウェア開発者向けの手法をまとめたフレームワークである SSDF への適合や SBOM の作成が求められている。米国におけるこうした流れを受け、経済産業省は SSDF の実装と SBOM の更なる活用促進について検討を進めている。
経済産業省	「IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)」の普及啓	業界及び企業において、「IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)」の活用が進むよう、

[54] JST(https://www.jst.go.jp/kisoken/crest/research_area/ongoing/bunya2021-2.html)
[55] 防衛装備庁(https://www.mod.go.jp/atla/funding/koubo/r07/r07koubo_full_hojo.pdf)
[56] サイバーセキュリティ 2025(2024 年度年次報告・2025 年度年次計画)
(https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025.pdf)

担当省庁	施策	概要
	発活動	普及啓発活動を行っている。
経済産業省 (IPA)	SCAP や CVSS の国際的な標準化活動への参画による情報システムの安全性確保及び国際動向の普及啓発	SCAP や CVSS の脆弱性対策に関する国際標準化活動に参画[57]するとともに、JVN iPedia を通じた脆弱性対策情報の発信[58]を行っている。
経済産業省 (JPCERT/CC)	脆弱性情報の提供、脅威・脆弱性マネジメントの重要性の啓発、及び脅威・脆弱性マネジメント支援	脆弱性情報を配信する VRDA (Vulnerability Response Decision Assistance)フィード[59]において HTML 形式や XML 形式での脆弱性情報の提供、また、「JPCERT/CC 四半期レポート」を通じた脅威・脆弱性に関する啓発活動を、関連する標準技術の変化を踏まえて実施している。
経済産業省	専門機関と連携したサイバーセキュリティ分野の国際標準策定の推進活動	専門機関と連携し、サイバーセキュリティの包括的な標準化を推進する ISO/IEC JTC1/SC27 等、主催の国際会合を通じて、日本の研究開発成果や IT 環境・基準を踏まえたサイバーセキュリティ分野の国際標準策定を推進している。
総務省	「クラウドサービス JPCERT/CC 提供における情報セキュリティ対策ガイドライン」の普及促進	クラウドサービス事業者がサービス提供時に実施するべき情報セキュリティ対策をまとめた「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及活動を実施している。本ガイドラインではネットワークにおける情報セキュリティ対策として Firewall や IDS、IPS の導入が推奨されている。

第４節　国内のサイバーセキュリティに関する倫理規制

倫理規制とは一般的に、個人や組織が社会的に望ましい行動をとるように導くための道徳的・社会的なルールや基準・規則と捉えることができる。本調査ではサイバーセキュリティ領域における倫理規制を、サイバー攻撃に対し個人や組織が社会的に望ましい行動を取るために定められた規範や原則、及びそれを担保する法的枠組みと捉える。特

[57] IPA(https://www.ipa.go.jp/security/vuln/scap/cvssv3.html)
[58] JVN iPedia(https://jvndb.jvn.jp/nav/jvndb.html)
[59] JPCERT(https://www.jpcert.or.jp/vrdafeed/)

に保護対象となる個人のプライバシーと国家や公共基盤の安全に関連する規制を以下の表 3-4-1 に示す。

表 3-4-1　サイバーセキュリティとの関連が認められる国内の倫理規制

規制	概要
個人情報保護法[60] (2003 年制定)	氏名や住所等の個人情報の取扱いに関する安全管理のルールを定め、個人の権利利益を保護するための基本法である。 本法律は、サイバー攻撃の検知や分析時、プライバシーを保護するために適用され得る。 サイバー攻撃検知に際し、利用される通信ログや IP アドレス等の情報が特定の個人を識別できる、又は他の情報と照合することにより個人を識別できる情報に該当する場合、本法律が対象になり得る。それらの情報を国外の SOC やクラウド解析基盤に送信する場合には、個人情報保護法上の越境移転規制が実務上問題となり得る。
電気通信事業法[61] (1984 年制定)	電気通信事業の適正な運営に関する必要な事項を定め、通信の秘密を保障する等、通信利用者の権利と公共性を確保するための法律である。 本法律は、サイバー攻撃の検知や分析時、プライバシーを保護するために適用され得る。 サイバー攻撃を検知する際においても、送信元や通信時間、通信回数等の監視は原則として認められず、通信の秘密を侵害しないよう実施することが求められる。
サイバーセキュリティ基本法[62] (2014 年制定)	サイバー攻撃の脅威に対応するため、国の責務や基本理念、サイバーセキュリティ戦略等を定め、国全体としてサイバーセキュリティ政策を推進するための基本法である。 具体的には国や、重要インフラ事業者に対し、サイバー攻撃への対応体制の整備、重大インシデント発生時の報告体制の確立等を定めている。 そのため本法は、サイバー攻撃から国家や公共基盤の安全を確保するために適用される。
サイバー対処能力強化法及び同整備法[63] (2025 年成立)	サイバー攻撃の高度化に対応し、官民連携及び通信情報の取得や利用に関する制度整備を通じ、国家としてのサイバー対処能力を強化するための新法である。 具体的には重要インフラ事業者等に対し、重大なサイバー攻撃の兆候や被害の発生時における政府への速やかな情報提供、平時か

[60] 個人情報の保護に関する法律(https://laws.e-gov.go.jp/law/415AC0000000057)
[61] 電気通信事業法(https://laws.e-gov.go.jp/law/359AC0000000086)
[62] サイバーセキュリティ基本法(https://laws.e-gov.go.jp/law/426AC1000000104)
[63] 重要電子計算機に対する不正な行為による被害の防止に関する法律
(https://laws.e-gov.go.jp/law/507AC0000000042)

規制	概要
	らの監視・連絡体制の整備、政府による対処方針に基づく協力等の対応が求められている。 そのため本法は、サイバー攻撃から国家や公共基盤の安全を確保するために適用される。

第５節　国外のサイバー攻撃検知に関する政策動向

国外におけるサイバー攻撃検知の政策動向は、米国・欧州・中国・韓国・イスラエルを中心として、国家レベルでのレジリエンス強化と先端技術を活用した防御能力の高度化を基軸に展開されている。米国・欧州は重要インフラ防護や国際協調を重視し、中国はサイバー主権の確立を掲げて国家統制的な安全保障体制を示している。韓国は北朝鮮情勢を背景とした積極的防衛への転換を進め、イスラエルは高度な技術優位性を基盤に国際的なサイバーレジリエンス構築を志向している。これらの政策は、それぞれの安全保障環境や産業構造に応じたアプローチを取りつつ、共通してサイバー攻撃の検知・分析・対応能力の強化を国家的課題として位置付けている。

１．　米国

米国は 2023 年に「国家サイバーセキュリティ戦略(National Cybersecurity Strategy)」[64]を策定し、サイバー空間における国家安全保障と経済活動の安定性確保を目的とした包括的な政策体系を構築した。同戦略は総額 175 億米ドル(約 2 兆 2,737 億円)の予算規模で推進され、国家・産業界・市民社会を横断する形でサイバーリスク低減とレジリエンス強化を図るものである。政府は「すべての米国民が恩恵を享受できる安全なデジタルエコシステムの確保」を中心理念として掲げ、サイバー攻撃の高度化・多様化に対応する体制整備を進めている。

本戦略では、サイバー攻撃の検知・防御を含む政策領域を 5 つの柱として整理している。第一に、重要インフラ防衛の強化として、電力・通信・医療等の基幹分野に対して最低限のサイバーセキュリティ要件を設定し、事業者によるセキュリティ実装の底上げを図る。第二に、脅威行動主体への対抗として、国家サイバー捜査ジョイントタスクフォース(JTF)を強化し、ランサムウェア集団や国家支援型攻撃者への対処力を拡充する。第三に、国全体のレジリエンス向上のため、ソフトウェア部品表(SBOM)の普及を推進し、ソフトウェア供給網全体の透明性と脆弱性管理の高度化を目指す。第四に、将来の安全保障基盤への投資として、ゼロトラストアーキテクチャの導入推進を掲げ、連邦政府機関のネットワーク防御の構造改革を進める。第五に、国際パートナーシップの構築では、国際サイバースペース・デジタルポリシー戦略を公表し、同盟国との連携強化や国際法執行協力の拡充を図る。

これらの取組は、攻撃検知・分析能力の高度化と、国全体での協調的セキュリティの確立を目的としたものであり、米国のサイバー政策の中心的基盤となっている。

[64] The National Cybersecurity Strategy (https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/)

第６節　各国における倫理規制

１．　米国

米国で定められているサイバー攻撃の検知や分析時、プライバシー保護のために適用され得る規制としては、Health Insurance Portability and Accountability Act[65]とGramm-Leach-Bliley Act[66]、California Consumer Privacy Act[67]/California Privacy Rights Act[68]が挙げられる。また、サイバー攻撃から国家や公共基盤の安全を確保するために適用され得る規則としては、Cyber Incident Reporting for Critical Infrastructure Act[69]とFederal Information Security Modernization Act[70]が挙げられる。

表 3-6-1　サイバーセキュリティとの関連が認められる米国の倫理規制

規制	概要
Health Insurance Portability and Accountability Act (1996 年制定)	医療機関や保険会社等に対し、患者の医療情報の適正な取扱いと安全管理を義務付ける米国の医療情報保護法である。 本法律は、サイバー攻撃の検知や分析時、プライバシー保護のために適用され得る。 サイバー攻撃検知の過程で取得分析される情報が、本法律の保護対象情報に該当する場合、利用・開示の正当性、最小限利用原則、安全管理措置の履行等が求められる。
Gramm-Leach-Bliley Act (1999 年制定)	銀行・証券・保険等の金融機関に対し、顧客の非公開個人情報の保護と情報セキュリティ対策を義務付ける法律である。 本法律は、サイバー攻撃の検知や分析時、プライバシー保護のために適用され得る。 サイバー攻撃検知の過程で取得分析される情報が、本法律の保護対象情報に該当する場合、事業者は情報共有に関するルール遵守、セキュリティ管理措置の実施等が求められる。
Federal Information Security Modernization Act (2014 年制定)	米国連邦政府機関及びその委託先に対し、情報システムのサイバーセキュリティ管理体制の整備を義務付ける法律である。 具体的には、連邦政府機関及び政府と契約関係にある事業者に対し、情報セキュリティ管理体制の構築及び継続的なリス

[65] Health Insurance Portability and Accountability Act (https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf)
[66] Gramm-Leach-Bliley Act(https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf)
[67] California Consumer Privacy Act(https://privacy.ca.gov/california-privacy-rights/rights-under-the-california-consumer-privacy-act/)
[68] California Privacy Rights Act(https://privacy.ca.gov/california-privacy-rights/rights-under-the-california-consumer-privacy-act/)
[69] Cyber Incident Reporting for Critical Infrastructure Act (https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf)
[70] Federal Information Security Modernization Act(https://www.govinfo.gov/app/details/PLAW-113publ283)

規制	概要
	ク管理を義務付ける連邦法であり、サイバー攻撃の検知、予防、監視及びインシデント対応計画の策定、定期的なリスク評価及び監査の実施が義務付けられている。そのため本法は、サイバー攻撃から国家や公共基盤の安全を確保するために適用される。
California Consumer Privacy Act (2018 年制定)	カリフォルニア州の消費者に、個人情報の開示や削除、第三者提供の拒否等の権利を保障する州法である。
California Privacy Rights Act (2020 年制定)	California Consumer Privacy Act of 2018 を改正し、個人情報の概念追加や独立監督機関の設置等を定めた州法である。 本法律は、サイバー攻撃の検知や分析時、プライバシー保護のために適用され得る。 サイバー攻撃検知の過程で取得分析される情報が、本法律の保護対象情報に該当する場合、利用目的を開示することや、本人が第三者への提供を拒否できる仕組みを整備することが求められる。
Cyber Incident Reporting for Critical Infrastructure Act (2022 年制定)	重要インフラ事業者に対し、重大なサイバーインシデント及び身代金支払を米国政府へ迅速報告することを義務付ける法律である。 具体的には重要インフラ事業者に対し、重大なサイバーインシデント発生時及びランサムウェア被害について、迅速報告義務を課す連邦法であり、攻撃検知から報告体制、証拠保全、初動対応までを事前に整備しておくことが定められている。 そのため本法は、サイバー攻撃から国家や公共基盤の安全を確保するために適用される。

２． 欧州

欧州(EU)で定められているサイバー攻撃の検知や分析時、プライバシー保護のために適用され得る規制としては、EU General Data Protection Regulation(Regulation 2016/679)[71]が挙げられる。また、サイバー攻撃から国家や公共基盤の安全を確保するために適用され得る規則としては、NIS Directive(Directive 2016/1148)[72]及び NIS2 Directive(Directive 2022/2555)[73]と、EU Cybersecurity Act(Regulation 2019/881)[74]が挙げられる。

[71] EU General Data Protection Regulation(Regulation 2016/679)
(https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng)
[72] NIS Directive(Directive 2016/1148)
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148&utm)
[73] NIS2 Directive(Directive 2022/2555)(https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng)
[74] EU Cybersecurity Act(Regulation 2019/881)
(https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng)

表 3-6-2　サイバーセキュリティとの関連が認められる欧州(EU)の倫理規制

規制	概要
Regulation 2016/679 (2016 年制定)	EU 域内の個人データ処理について包括的な保護ルールを定め、域外事業者にも適用される統一的な個人情報保護規則である。 本規則は、サイバー攻撃の検知や分析時、プライバシー保護のために適用され得る。 サイバー攻撃検知の過程で取得・分析される通信ログ、IP アドレス、端末識別子等が個人データに該当する場合、その収集、保存、分析及び第三者提供に対して制限を課す規則である。具体的には、データ処理の適法性や目的限定原則、データ最小化原則、保存期間制限、適切な安全管理措置等が義務付けられており、サイバー攻撃検知を目的とする場合であっても、必要最小限の範囲でのみデータを取得・利用することが要求される。
Directive 2016/1148 (2016 年制定)	重要サービス事業者及びデジタルサービス事業者に対し、サイバーセキュリティ対策とインシデント報告義務を課す包括的なサイバーセキュリティ指令である。
Directive 2022/2555 (2022 年制定)	Directive (EU) 2016/1148 を全面改正し、対象事業者の拡大、管理責任の強化、厳格なインシデント報告義務等を導入した EU の新サイバーセキュリティ指令である。 具体的にはエネルギー、交通、金融、医療、行政機関等の重要事業者に対し、サイバーリスク管理体制の整備、技術的・組織的安全対策の実施、重大インシデント時の報告義務が定められている。 そのため本指令は、サイバー攻撃から国家や公共基盤の安全を確保するために適用される。
Regulation 2019/881 (2019 年制定)	ICT 製品やサービス、プロセスに関し EU 共通のサイバーセキュリティ認証制度を創設した規則である。 具体的には、サイバーセキュリティ製品を含むネットワーク機器や ICT サービス等を対象として、一定のセキュリティ水準を第三者認証により証明できる任意の認証制度の枠組みを定めている。 そのため本規則は、サイバー攻撃から国家や公共基盤の安全を確保するために寄与する。

第 7 節　国際標準化団体の取組・内容

国際的な規格の策定に携わる国際標準化団体は、専門委員会やワーキンググループを通じて、検知技術に関連する標準化を進めている。特にサイバー攻撃検知技術に関する規格の策定を進めている団体及びその団体の取組を表 3-7-1 に示している。

表 3-7-1　国際標準化団体の取組・内容

団体名	取組
ISO	ISO は多岐にわたる分野で規格の策定を行っている。サイ

団体名	取組
	バーセキュリティの分野では、ISO は後述の IEC と連携し、情報技術分野での標準化を進める合同技術委員会である JTC 1 を設立した。JTC 1 に設置されている情報セキュリティに関する標準化を行う分科委員会の SC(Sub-Committee)27[75]において、後述の ISO/IEC27039:2015 をはじめとしたサイバーセキュリティ検知に関する標準化活動も行われている。
IEC	IEC は電気、電子及び関連技術の分野における規格の策定[76]を行っている。サイバーセキュリティの分野では、IEC は ISO と連携し、情報技術分野での標準化を進める合同技術委員会である JTC 1 を設立した。JTC 1 に設置されている情報セキュリティに関する標準化を行う分科委員会の SC27 において、後述の ISO/IEC 27039:2015 をはじめとしたサイバーセキュリティ検知に関する標準化活動も行われている。
IETF	IETF はインターネット技術における規格の策定[77]を行っている。IETF は様々な分野に分かれて活動を行っており、各分野にはワーキンググループが複数存在している。IETF が活動を行う分野にはセキュリティ分野も存在しており、認証技術や暗号技術をはじめとしたワーキンググループが複数存在[78]している。過去には侵入検知の交換フォーマットに関するワーキンググループも存在しており、侵入検知システム間でやり取りが行われるデータフォーマットの策定[79]を行っていた。
OASIS	OASIS は情報交換技術に関する規格を発行している。 OASIS では人工知能やブロックチェーンをはじめとした様々なプロジェクトが実施[80]されている。サイバーセキュリティの分野では、脅威インテリジェンスの共有をサポートするプロジェクト[81]や組織のセキュリティ対策の促進を図るプロジェクト[82]等が行われている。
ITU	ITU は通信分野における規格の策定を行っている。サイバーセキュリティの分野では、電気通信標準化部門である

[75] 情報セキュリティ白書 2025(https://www.ipa.go.jp/publish/wp-security/j5u9nn0000004wk0-att/ISWP2025_Chap4.pdf)
[76] JISC(https://www.jisc.go.jp/international/iec-guide.html)
[77] IETF(https://www.ietf.org/about/introduction/)
[78] IETF(https://datatracker.ietf.org/group/sec/about/)
[79] IETF(https://datatracker.ietf.org/wg/idwg/about/)
[80] OASIS(https://www.oasis-open.org/org/)
[81] OASIS(https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=c6c33da0-d1ee-42dd-9427-018dc7d32277)
[82] OASIS(https://www.oasis-open.org/tc-cacao/)

団体名	取組
	ITU-T に研究グループである SG17 が設置[83]されており、セキュリティ関連の標準化活動を進めている。また、Recommendation X.1375 (10/20)をはじめとしたサイバーセキュリティ検知に関する規格も SG17 で策定されている。

第８節　各国で採用・検討されている規格及び／又は標準化の取組・内容

１．日本

日本における標準化活動は、国際的な規格との整合性を保ちつつ、国内の産業や社会のニーズに応じた規格の策定と普及を目的として進められている。このような流れを受け、日本国内では、標準化を推進する主要な団体である JISC や、各官公庁の管轄下にある関連団体が、標準化活動を進めている。

（１）　JISC

JISC は経済産業省の下に設置されている審議会である。ISO 及び IEC に対する日本の会員として、国際規格の開発に参加[84]している。サイバーセキュリティ分野では、情報セキュリティマネジメントシステムに関する ISO/IEC 27000 シリーズや、IT セキュリティ評価基準である ISO/IEC 15408 に対応する国内向けの規格の策定を進めている。具体的には、JIS X 5070-1:2011[85]は IT セキュリティ評価の国際規格である ISO/IEC 15408-1:2009 と対応させた規格であり、IT 製品のセキュリティ特性を評価することを目的としている。

（２）　IPA

IPA は「サイバーセキュリティの確保」「デジタル人材の育成」「デジタル基盤の提供」の 3 つを事業基盤として、IT 社会の発展に向けた技術と人材の強化[86]を行っている。サイバーセキュリティ分野では、J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)を発足させ、サイバー攻撃に関する情報共有[87]を進めている。さらに IPA は、ISO/IEC 15408 に基づいた JISEC(Japan Information Technology Security Evaluation and Certification Scheme)の認証機関として、IT セキュリティ評価及び認証制度の運用[88]を担っている。加えて、コンピュータ不正アクセスやウイルスによる被害を抑えるための「情報セキュリティ早期警戒パートナーシップガイドライン」[89]や、製品開発者向けに脆弱性対処のための項目を整理した「脆弱性対処に向けた製品開発者向けガイド」[90]を公開しており、企業に対して実務上有益な情報提供を行っている。

---

[83] ITU(https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx)
[84] JISC(https://www.jisc.go.jp/jisc/index.html)
[85] JISC
(https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?toGnrJISStandardDetailList)
[86] IPA(https://www.ipa.go.jp/about/nl10bi000000favk-att/jigyoannai.pdf)
[87] IPA(https://www.ipa.go.jp/security/j-csip/about.html)
[88] IPA(https://www.ipa.go.jp/security/jisec/index.html)
[89] IPA(https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html)
[90] IPA(https://www.ipa.go.jp/security/guide/vuln/forvendor.html)

（３） NICT

NICT は ICT 分野における研究開発の推進を目的として活動[91]している。NICT 内にはサイバーセキュリティ研究所が設置[92]されており、専門的な研究が進められている。具体的には、総務省や ICT-ISAC との連携により、IoT 機器のセキュリティ対策を強化することを目的とした「NOTICE」プロジェクト[93]が推進されている。このプロジェクトでは、サイバー攻撃に利用されている可能性のある IoT 機器を特定し、IoT 機器の管理者や利用者に対して注意喚起を実施することで、サイバー攻撃の発生及び被害の防止を図っている。また、NICT では、サイバー攻撃関連通信の観測及び分析を行う「NICTER」プロジェクト[94]も展開されている。この取組では、インターネット上の不審な通信を観測及び分析することで、サイバーセキュリティ対策の強化を目指している。

２． 米国

米国は、国際規格を踏まえた規格を策定すると同時に、米国の政府機関でも運用されるフレームワークの策定・公開も進めている。米国内でサイバー攻撃検知技術の標準化を推進する主な団体としては ANSI や NIST、MITRE が挙げられ、国際規格の採用やフレームワークの策定を通じて標準化活動を展開している。

（１） ANSI

ANSI は ISO 及び IEC における米国代表機関としての役割を担っている。米国の標準を国際的に普及させるとともに、国際標準を国内に導入する活動を推進している。ただし、ANSI 自体は規格を開発しておらず、ANSI が認定した組織により開発された規格の承認[95]を行っている。サイバーセキュリティの分野では、ANSI が認定した機関である INCITS が INCITS/ISO/IEC 27039:2015(R2022)を発表している。これは侵入検知・防止システム(IDPS)の選定・導入・運用方法を示した規格である ISO/IEC 27039:2015 を採用した規格[96]であり、米国内での規格利用の促進を図っている。

[91] NICT(https://www.nict.go.jp/about/)
[92] NICT(https://www.nict.go.jp/about/organization.html)
[93] NOTICE(https://notice.go.jp/about)
[94] NICTER(https://www.nicter.jp/)
[95] ANSI(https://ansi.org/standards-faqs#us-system)
[96] ANSI(https://webstore.ansi.org/standards/incits/incitsisoiec270392015r2022)

（２） NIST

NIST は米国商務省傘下の研究機関であり、技術の進歩による米国の産業競争力向上[97]を目指している。NIST には複数の研究所が存在しており、その中の 1 つである ITL がサイバーセキュリティに関するフレームワーク等の策定を担当[98]している。NIST が策定した CSF は、脅威の侵入を防ぐ事前対策に加え、侵入後の検知、対応、復旧といった事後対策も含む広範な管理策を提供している。2024 年に公開された CSF 2.0 では、業界や規模を問わず、あらゆる組織での利用が進むように再設計[99]されている。また、米国の政府機関のセキュリティ対策を拡充させるために、NIST は SP800 シリーズと呼ばれるガイドラインを発行[100]している。例えば SP800 シリーズにはサイバー攻撃検知に関わるものとして NIST SP 800-94 が存在[101]しており、組織における IDPS の導入から運用までを支援するための指針が示されている。

（３） MITRE

MITRE は米国で設立された非営利組織であり、サイバーセキュリティをはじめとした幅広い分野に対して知見を提供[102]している。サイバーセキュリティの分野において、MITRE が策定した ATT&CK[103]は、攻撃者の行動をフェーズごとに分類し、攻撃者の戦術や技術、手法を体系的にまとめたフレームワークである。この ATT&CK を補完する形で、MITRE はサイバー攻撃に対する対応策に焦点を当てたフレームワークである D3FEND[104]を策定し、セキュリティシステムの設計者等に対して、サイバー攻撃に対する防御施策に関する体系的な知識を提供している。

[97] NIST(https://www.nist.gov/about-nist)
[98] NIST(https://www.nist.gov/laboratories)
[99] NIST(https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)
[100] IPA(https://www.ipa.go.jp/security/reports/oversea/nist/nist_publications.html)
[101] NIST(https://csrc.nist.gov/pubs/sp/800/94/final)
[102] MITRE(https://www.mitre.org/who-we-are/our-story)
[103] MITRE(https://attack.mitre.org/)
[104] MITRE(https://d3fend.mitre.org/faq/)

第４章　特許動向調査

第４章では、サイバー攻撃検知技術に関する特許動向調査の結果を示す。

要約

第４章の要約

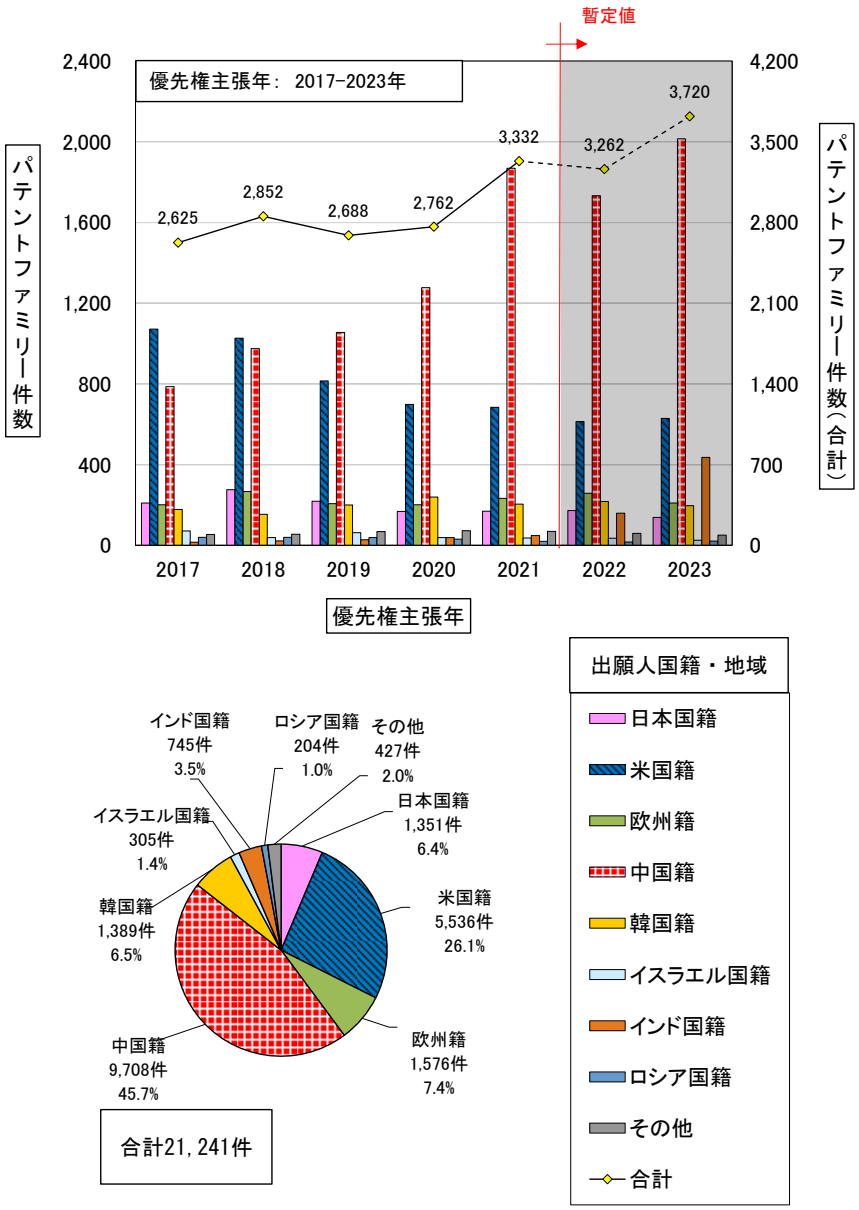
- 調査対象国におけるサイバー攻撃検知技術に関するパテントファミリー件数(調査期間：2017 年から 2023 年)は、2017 年から 2020 年まではほぼ横ばいで推移していたが、2021 年以降は増加傾向が認められた。2017 年のパテントファミリー件数は 2,625 件だが、2021 年には 3,332 件になり、暫定値ではあるが 2023 年は 3,720 件に達している。【図 4-1-1】
- 出願人の国籍・地域別のパテントファミリー件数は、中国籍(世界シェア 45.7%)が最も多く、次いで米国籍(26.1%)、欧州籍(7.4%)、韓国籍(6.5%)、日本国籍(6.4%)、インド国籍(3.5%)の順となっている。【図 4-1-1】
- 中国籍の出願人によるパテントファミリー件数は、調査期間を通じておおむね増加傾向にあり、2021 年には 2017 年の 2 倍以上に達している。一方で米国籍の出願人によるパテントファミリー件数は減少傾向にあり、2017 年は米国籍が中国籍を上回っていたが、2019 年に逆転し、2021 年には中国籍が米国籍の 2 倍以上となっている。日本国籍、欧州籍、韓国籍の出願人によるパテントファミリー件数は、調査期間中大きな増減なく推移している。インド国籍の出願人によるパテントファミリー件数は、2017 年から 2021 年にかけて緩やかに増加していたが、2022 年以降急激に増加している。暫定値ではあるが、2023 年は中国、米国に次いでインドが調査国中 3 位となっている。【図 4-1-1】
- 日本国籍の出願人による出願先国を出願件数で比較すると、日本(1,137 件)、米国(789 件)、中国(253 件)、欧州(231 件)、韓国(21 件)の順となっている。【図 4-1-2】
- 出願人の自国出願比率を出願人の国籍・地域別に比較すると、日本国籍は 46%であるのに対し、米国籍(63%)、中国籍(93%)、韓国籍(65%)は、半数以上が自国に出願されている。中国籍の出願人は、自国内での特許取得を重視していることが読み取れる。一方、欧州籍の自国出願比率は 28%、イスラエル国籍は 6%と共に低く、自国よりも国外での特許取得を重視しているといえる。【表 4-4-1】
- 侵入／異常検知技術のうち、DoS/DDoS 攻撃、電子メール経由、フィッシング、ランサム攻撃、サプライチェーン攻撃、サイドチャネル攻撃を手口とする侵入／異常の検知技術は、米国籍が首位であり、全体の件数では首位である中国籍よりも優位である。中国籍は、ポートスキャン及び脆弱性からの侵入で首位である。また、インド国籍は、ゼロデイ攻撃及び AI を利用した攻撃で首位である。【図 4-2-1】
- ウイルス／マルウェア検知技術のうち、電子メール配布、ボットネット／踏み台、ゼロデイ攻撃、サプライチェーン攻撃を感染経路とするウイルス／マルウェアの検知技術は、米国籍が首位である。中国籍は Web サイト配布及び脆弱性からの感染で首位であり、インド国籍は AI を利用した感染で首位である。【図 4-2-2】
- 特定の産業分野向けのサイバー攻撃検知技術については、電力分野で中国籍出願人のパテントファミリー件数が 325 件と最も多く、調査国中 2 位の米国籍出願人の 88 件を大きく上回っている。金融分野でも中国籍が 357 件で首位、米国籍が 273 件で続き、この 2 カ国が突出している。3 位の欧州籍は 50 件にとどまる。【図 4-2-5】

- 車両分野では日本国籍が 271 件で首位、米国籍(198 件)、中国籍(191 件)、欧州籍(183 件)で続いている。製造分野では中国籍の 267 件が最も多く、次いで米国籍(162 件)、日本国籍(153 件)、欧州籍(135 件)となっている。【図 4-2-5】
- 車両分野及び製造分野における日本の技術力マップの拡大係数(成長度を示す指標)は調査国平均を下回っており、この傾向が続けば拡大係数の高い中国、韓国、インド等に追い抜かれる可能性がある。【図 4-2-6】～【図 4-2-13】
- パテントファミリー件数の上位 10 者はすべて米国企業及び中国企業であり、20 位以内に入る日本企業は日本電気と NTT の 2 社のみである。一方、国際パテントファミリー件数で見ると、日本電気と NTT がそれぞれ 4 位、5 位に入り、上位 10 者のうち中国企業は 2 位の華為技術のみとなる。これは中国企業が自国内での出願に重点を置く傾向が強いためと考えられる。【表 4-3-1】【表 4-3-2】

第１節　全体動向調査

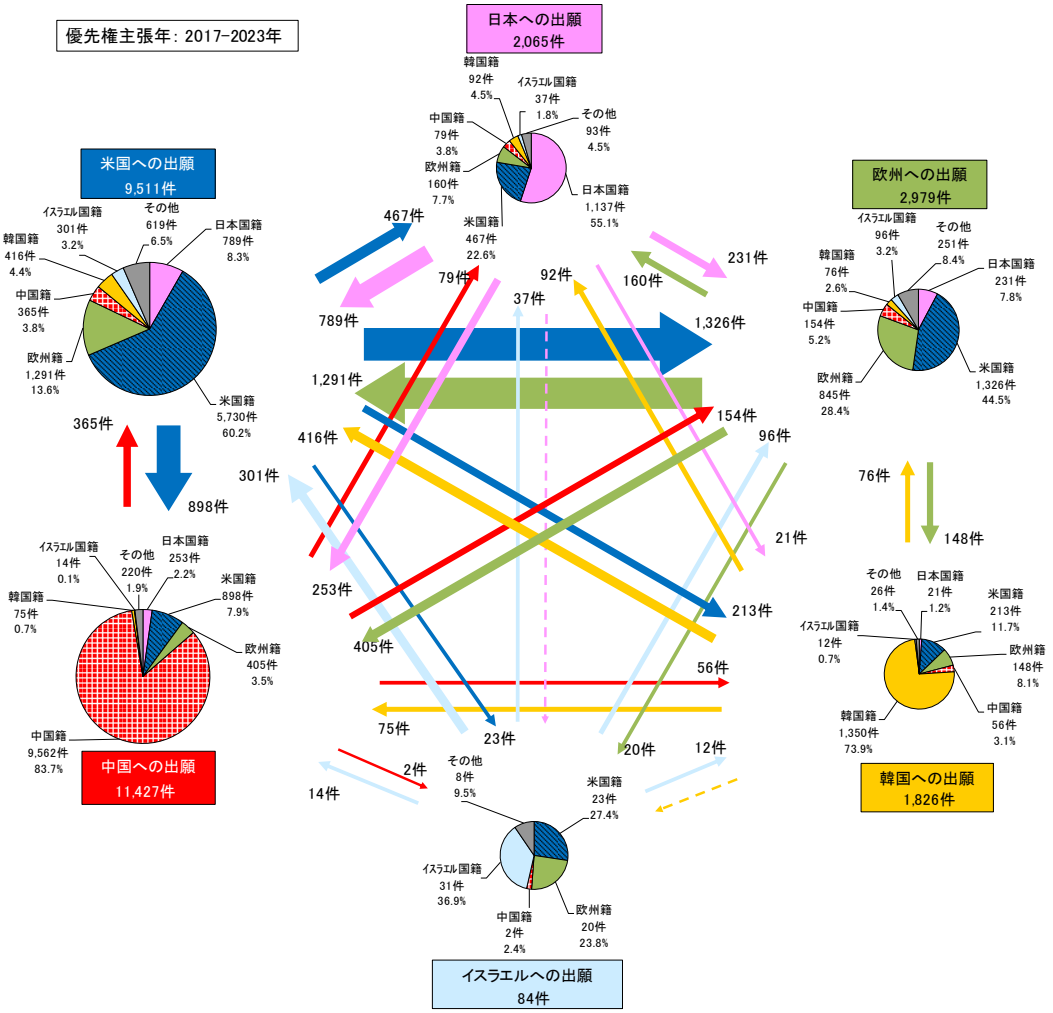
本節では、特許動向調査のうち全体動向調査の結果を示す。ファミリー単位及び出願単位にて、出願人国籍・地域、出願先国・地域、出願人属性等を基に分析している。なお、パテントファミリーのうち日本語・英語・中国語・韓国語の一次文献の順に代表文献を選定した。

図 4-1-1　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図 4-1-2　［出願先：日米欧中韓以］［出願先国・地域別］［出願人国籍・地域別］出願件数収支



※件数が 0 件の場合、当該矢印を点線で示している。

要約

第２節　技術区分別動向調査

本節では、特許動向調査のうち技術区分別動向調査の結果を示す。ファミリー単位及び出願単位にて、技術区分、出願人国籍・地域、出願先国・地域等を基に分析している。

図 4-2-1　［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］パテントファミリー件数（大区分：侵入／異常検知、優先権主張年：2017-2023 年）

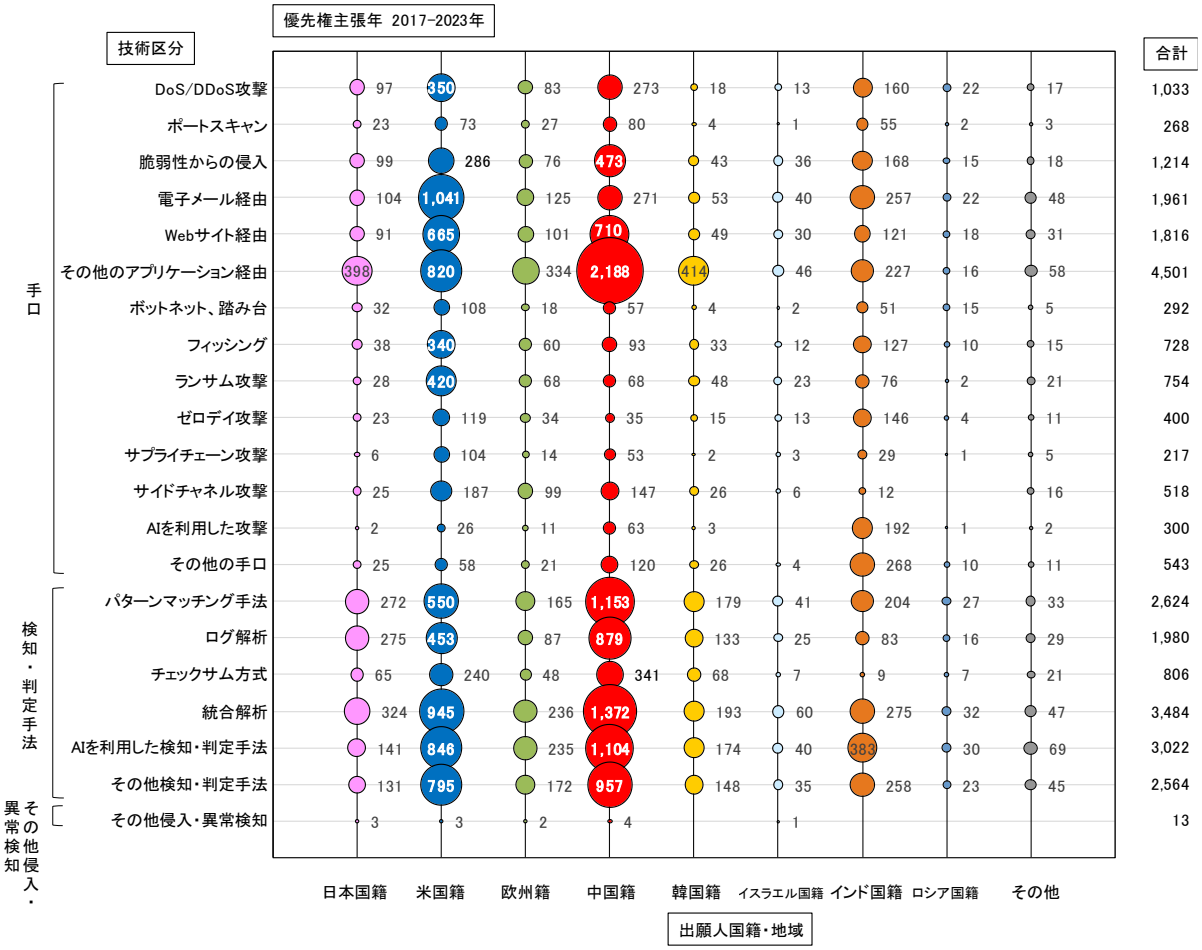


図 4-2-2　[出願先：日米欧中韓以印露 WO][技術区分別－出願人国籍・地域別] パテントファミリー件数（大区分：ウイルス／マルウェア検知、優先権主張年：2017-2023 年）

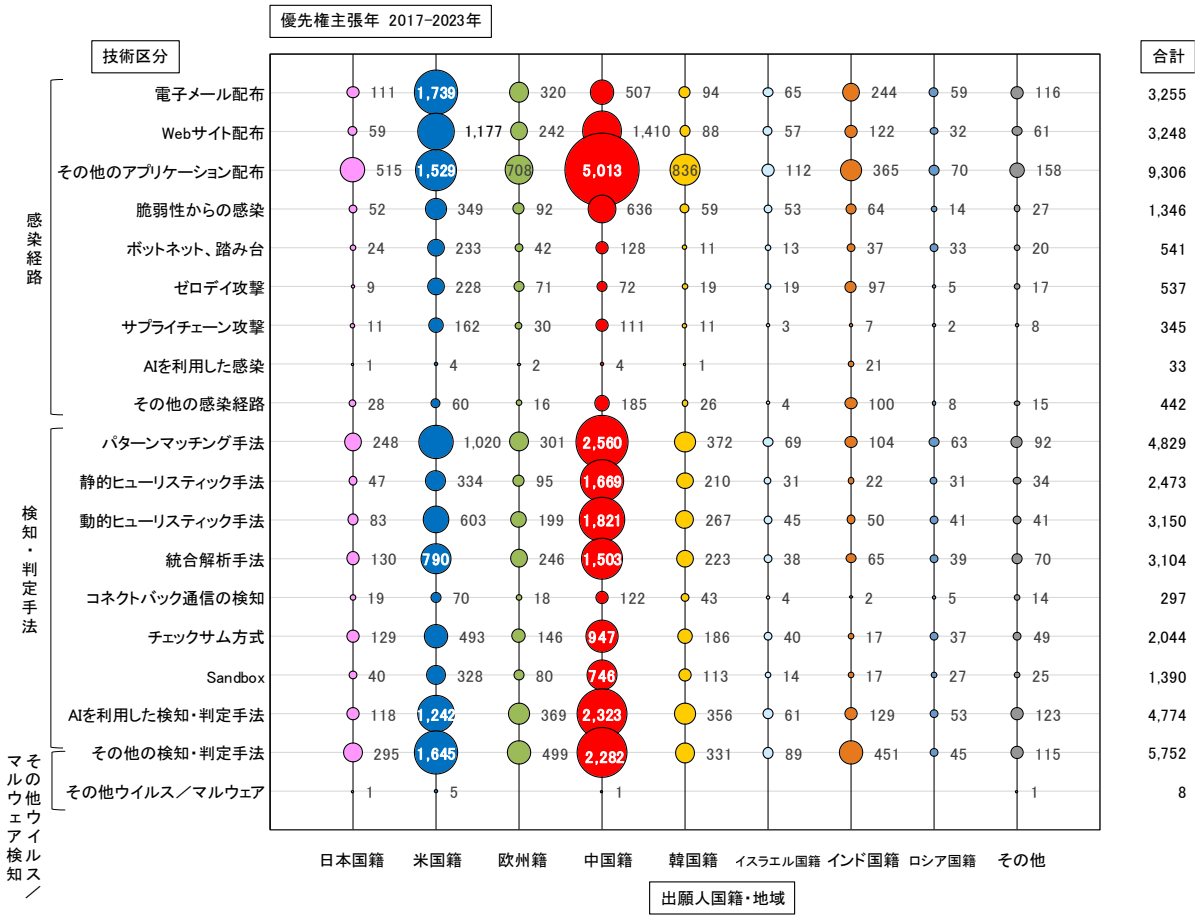


図 4-2-3　［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］パテントファミリー件数（大区分：検知共通、その他（検知）、優先権主張年：2017-2023 年）

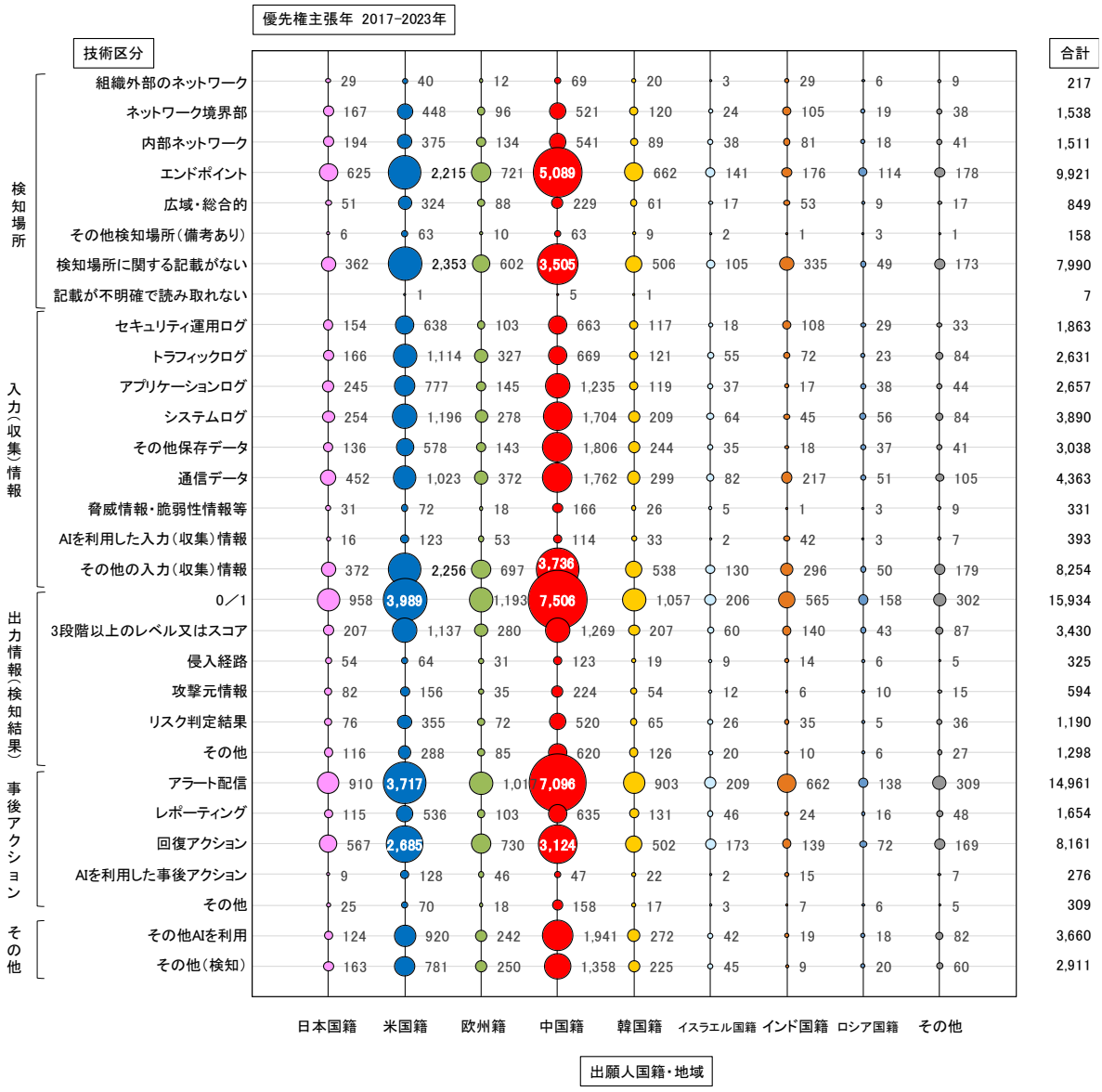


図 4-2-4　［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］パテントファミリー件数（大区分：適用領域（産業等）、解決課題／効果、AI に対する攻撃対策、脅威インテリジェンス、優先権主張年：2017-2023 年）

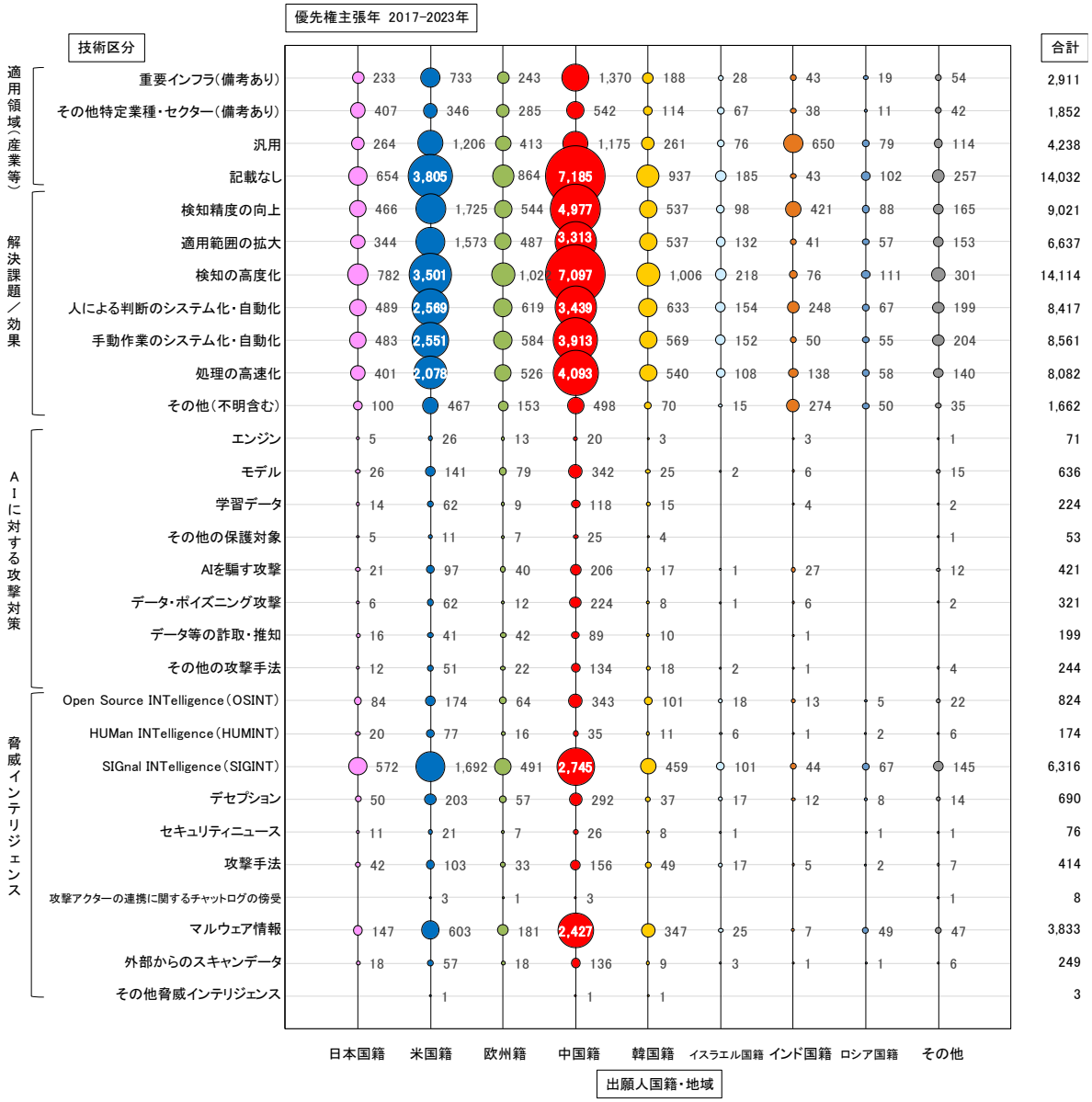


図 4-2-5　［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］パテントファミリー件数（重要インフラ、その他特定業種・セクター、優先権主張年：2017-2023 年）

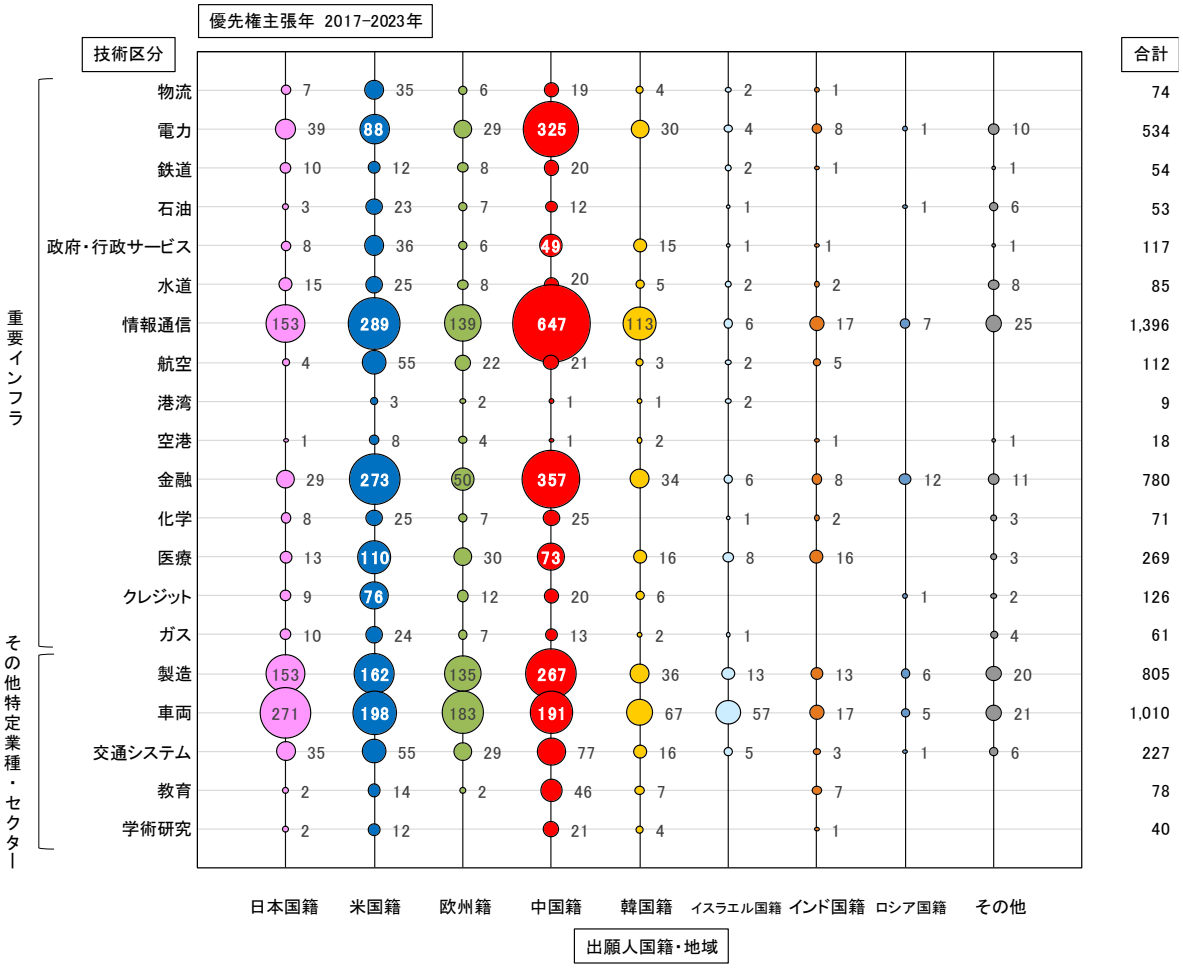
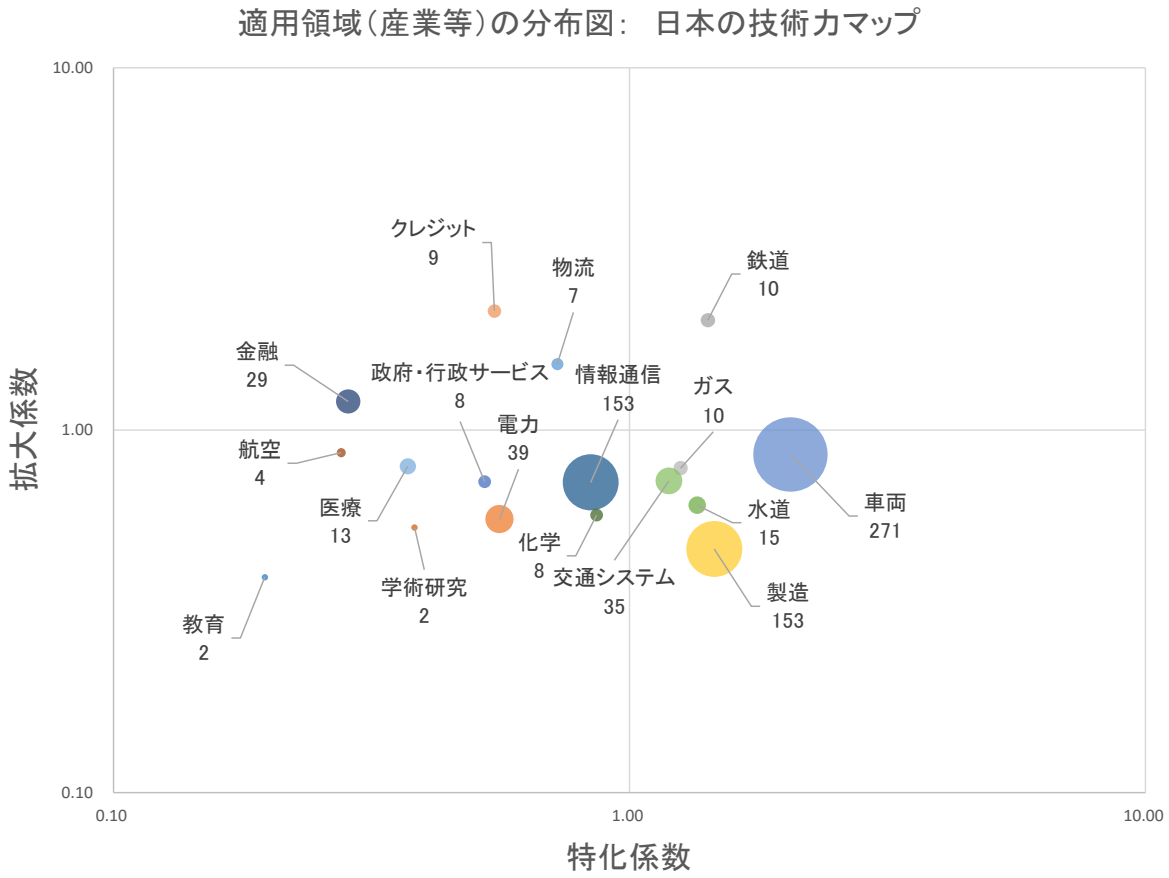


図 4-2-6　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝日本)

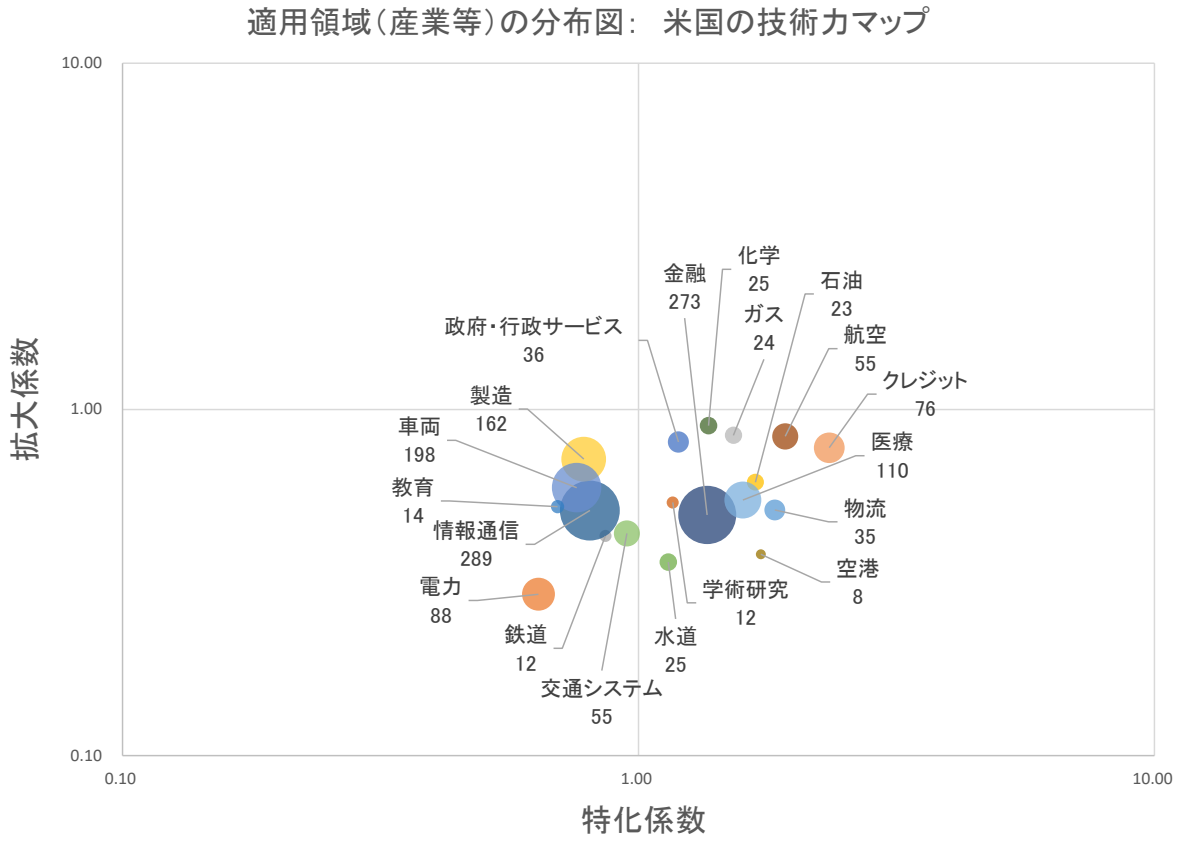
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-7　［出願先：日米欧中韓以印露 WO］［技術区分別］縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図（技術区分＝適用領域（産業等）、出願人国籍・地域＝米国）

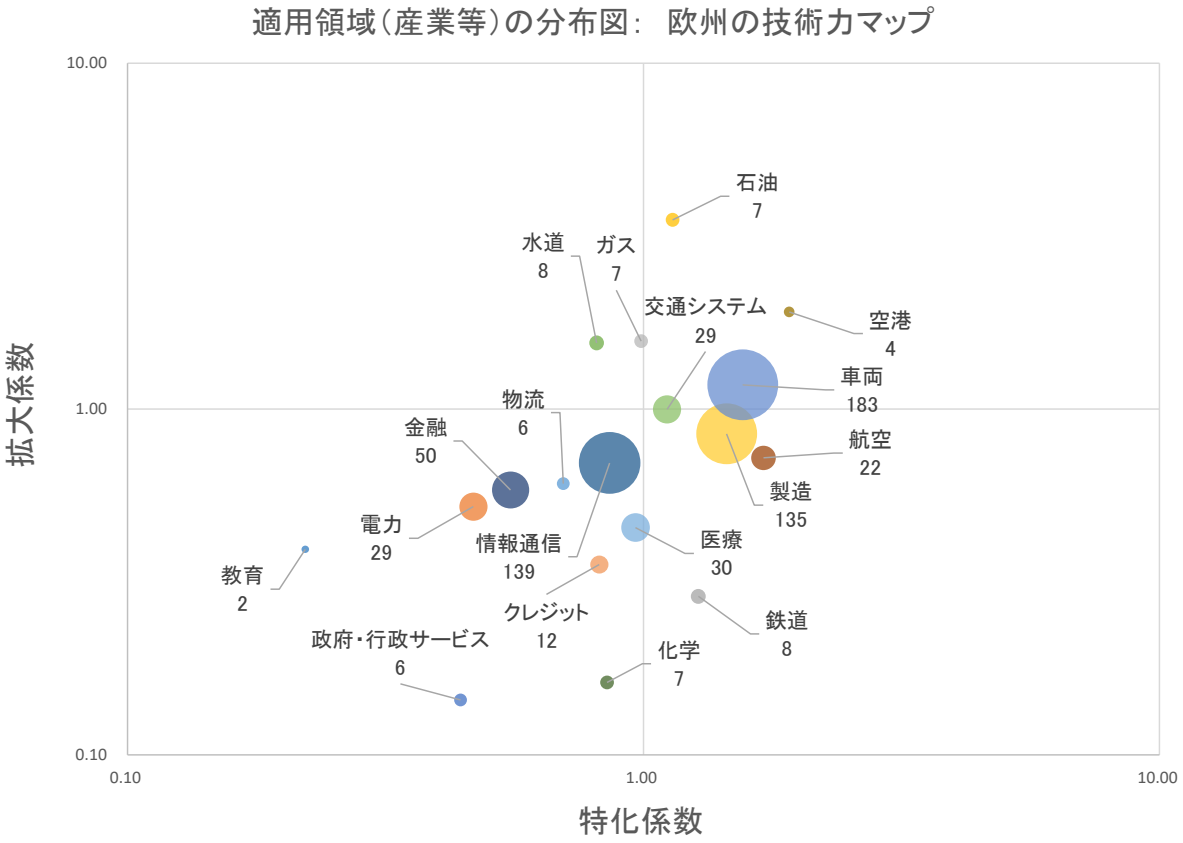
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-8　［出願先：日米欧中韓以印露 WO］［技術区分別］縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図（技術区分＝適用領域（産業等）、出願人国籍・地域＝欧州）

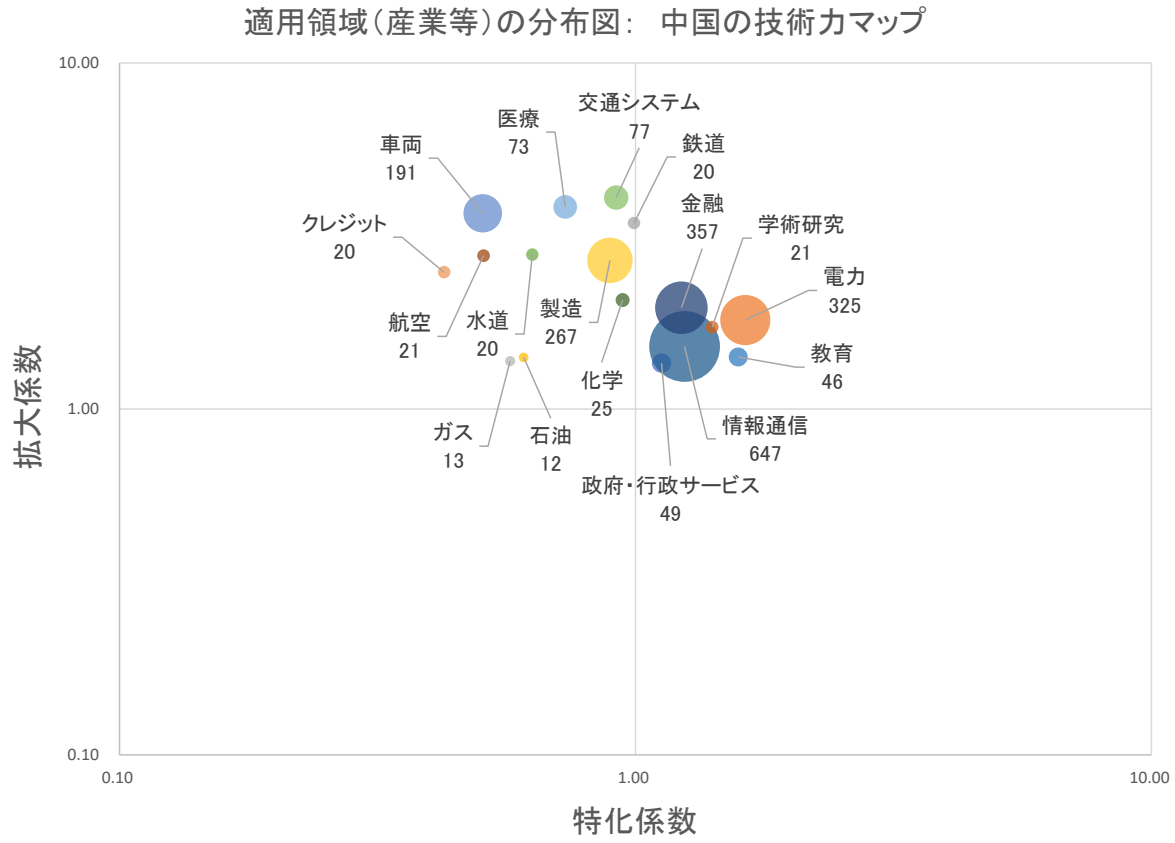
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-9　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝中国)

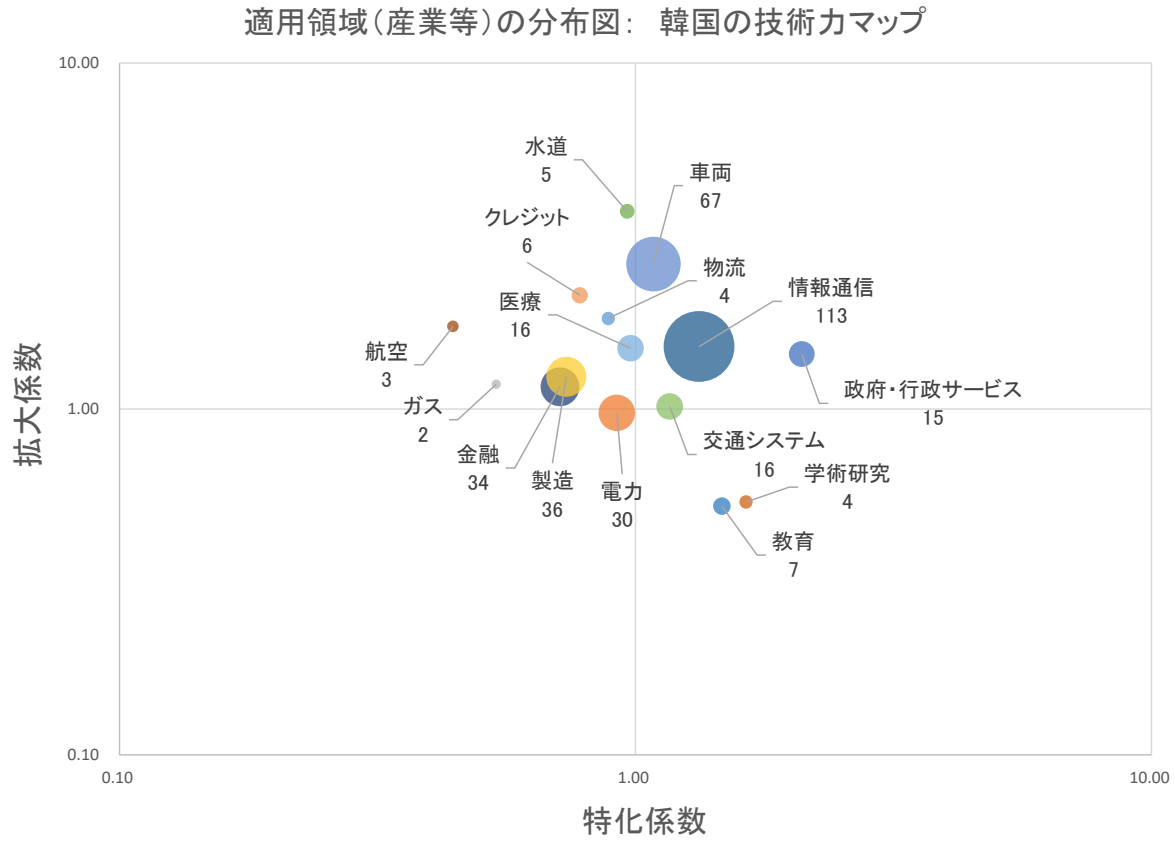
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-10　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝韓国)

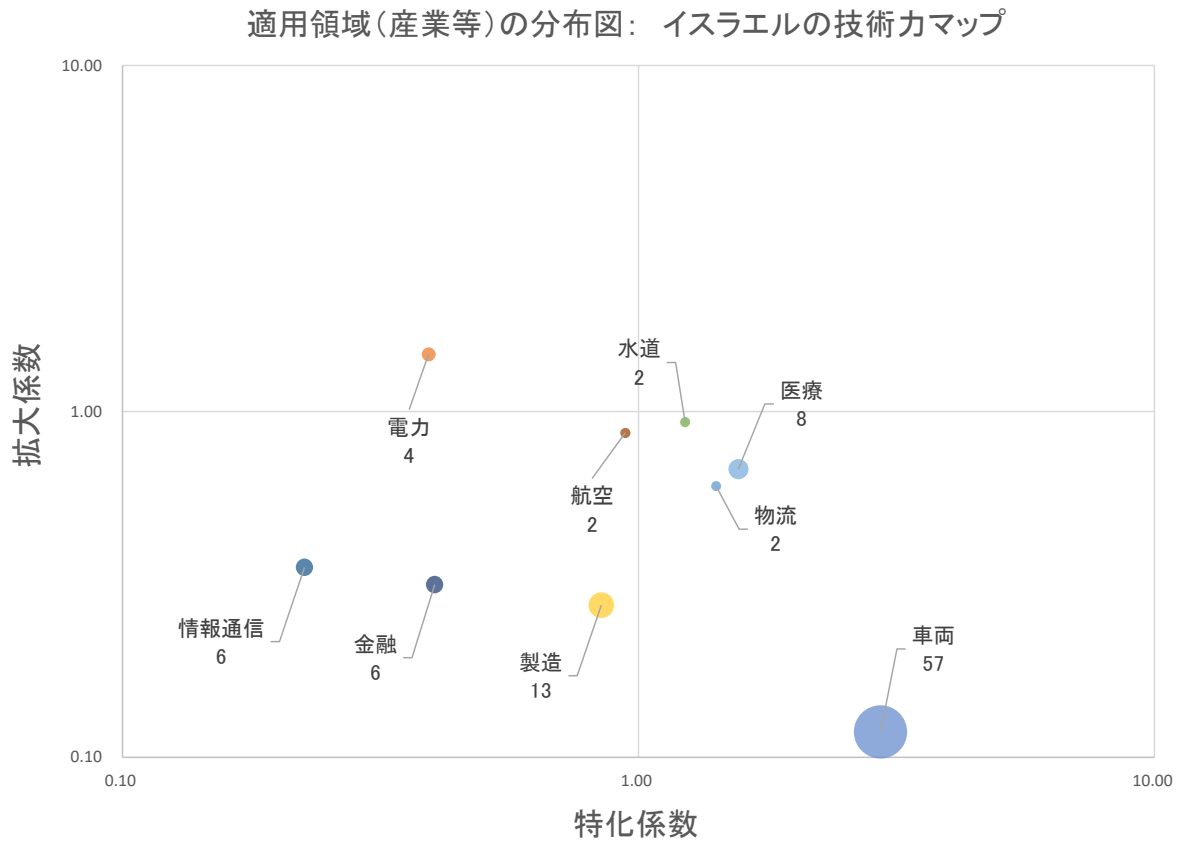
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-11　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝イスラエル)

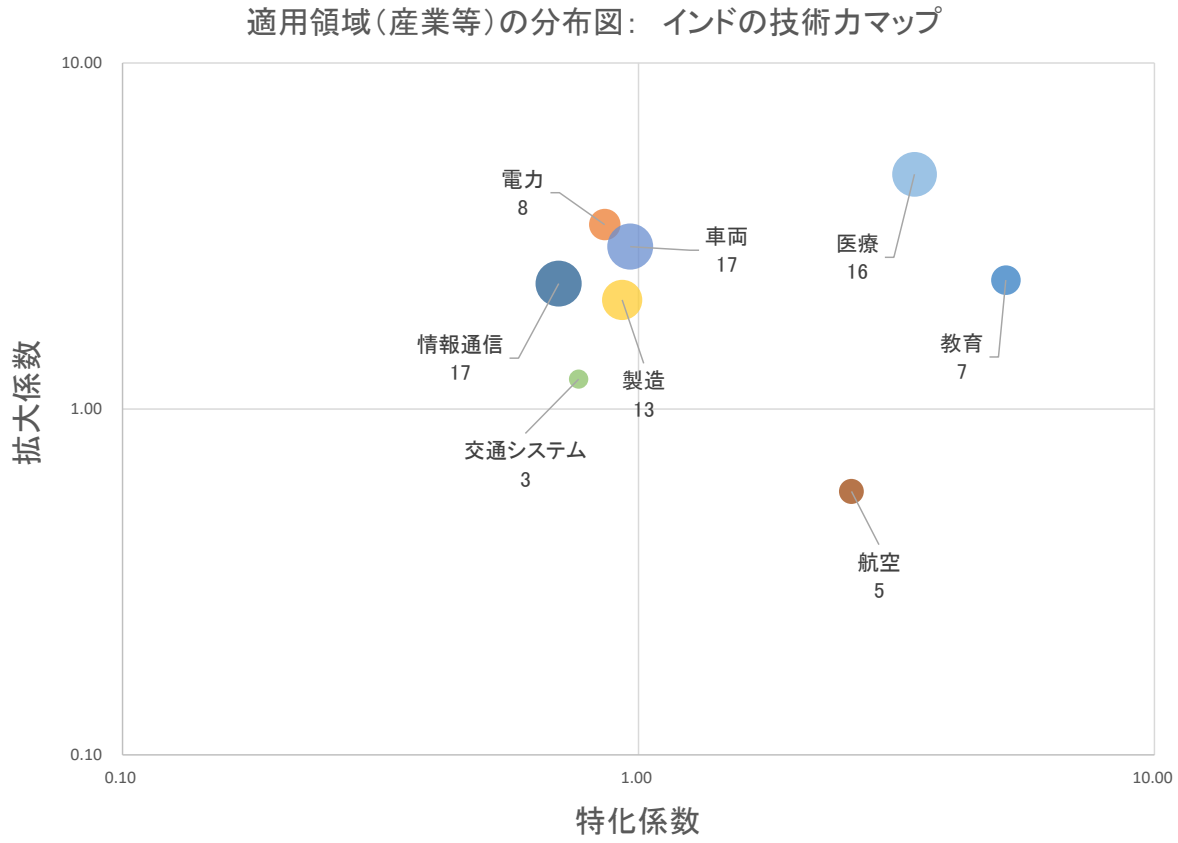
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-12　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝インド)

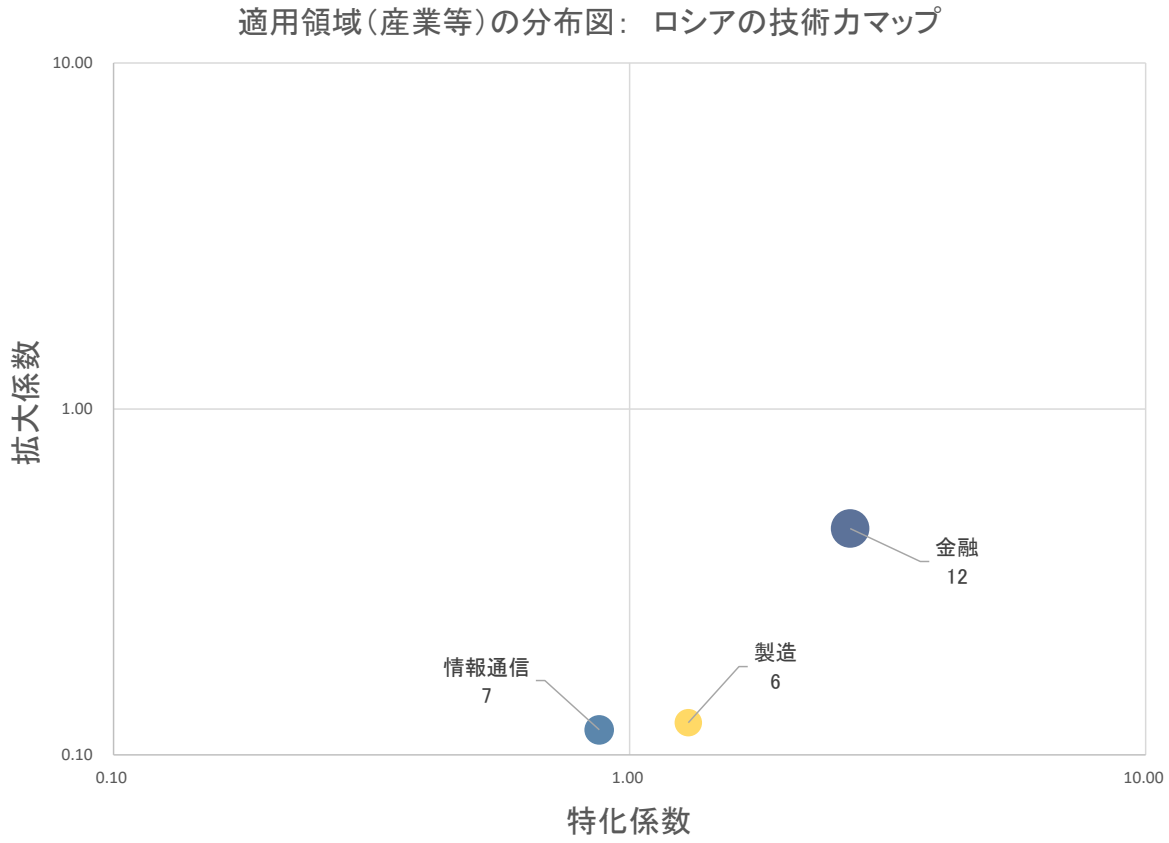
優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

図 4-2-13　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域（産業等)、出願人国籍・地域＝ロシア)

優先権主張年　2017-2023年



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

第３節　出願人別動向調査

本節では、特許動向調査のうち、パテントファミリー件数、国際パテントファミリー件数の出願人ランキングを示す。

表 4-3-1　［出願先：日米欧中韓以印露 WO］パテントファミリー件数上位出願人ランキング

順位	出願人名称	ファミリー件数
1	IBM株式会社（米国）	394
2	マイクロソフト株式会社（米国）	374
3	北京安天网络安全技术有限公司（中国）	297
4	インテル株式会社（米国）	280
5	国家電網公司（中国）	272
6	テンセント合同会社（中国）	252
7	サングフォーテクノロジズ株式会社（中国）	237
8	華為技術株式会社（中国）	220
9	SUZHOU INSPUR INTELLIGENT TECHNOLOGY（中国）	201
10	デル・テクノロジーズ株式会社（米国）	198
11	アリババ 株式会社（中国）	196
12	チー・アン・シン・テクノロジー株式会社（中国）	192
13	チットカーラ大学（インド）	178
14	日本電気株式会社	177
14	ヒューレット・パッカード合同会社（米国）	177
16	DBAPPセキュリティ（中国）	173
17	QIZHI SOFTWARE BEIJING（中国）	166
18	トップセック・テクノロジーズ株式会社（中国）	165
19	NTT株式会社	158
20	バンク・オブ・アメリカ株式会社（米国）	153

表 4-3-2　［出願先：日米欧中韓以印露 WO］［IPF］国際パテントファミリー件数上位出願人ランキング

順位	出願人名称	IPF件数
1	マイクロソフト株式会社（米国）	307
2	華為技術株式会社（中国）	149
3	インテル株式会社（米国）	130
4	日本電気株式会社	129
5	NTT株式会社	122
6	ボッシュ株式会社（ドイツ）	113
7	IBM株式会社（米国）	112
8	株式会社カスペルスキー（ロシア）	102
9	ヒューレット・パッカード合同会社（米国）	99
10	サムスン電子株式会社（韓国）	97
11	パナソニック株式会社	88
11	シーメンスAG（ドイツ）	88
13	株式会社日立製作所	71
14	三菱電機株式会社	68
15	クラウドストライク株式会社（米国）	67
16	アリババ 株式会社（中国）	66
16	ブリティッシュ・テレコミュニケーションズ plc （イギリス）	66
18	グーグル合同会社（米国）	65
19	パロアルトネットワークス株式会社（米国）	60
20	シスコシステムズ合同会社（米国）	50

第４節　総合分析に関する調査

本節では、特許動向調査のうち総合分析に関する調査の結果を示す。本調査では、第１節から第３節までの調査以外に総合分析のために追加で調査した図表を図示した。

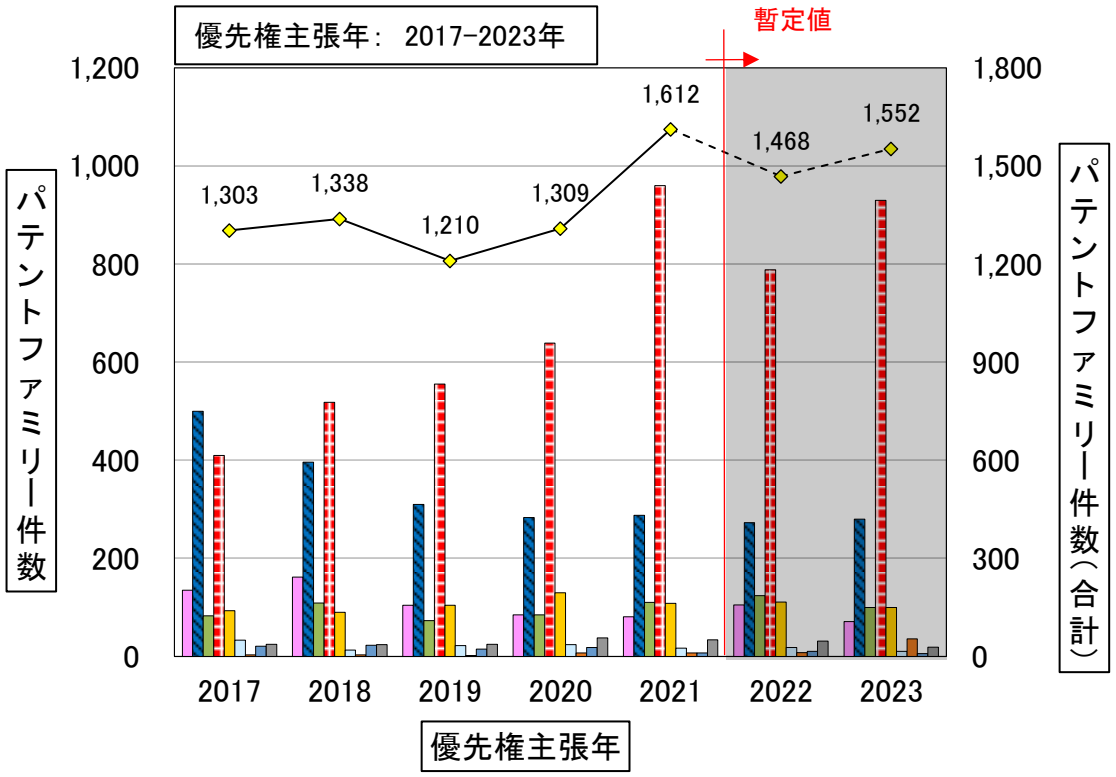
表 4-4-1　［出願人国籍・地域別］自国出願比率

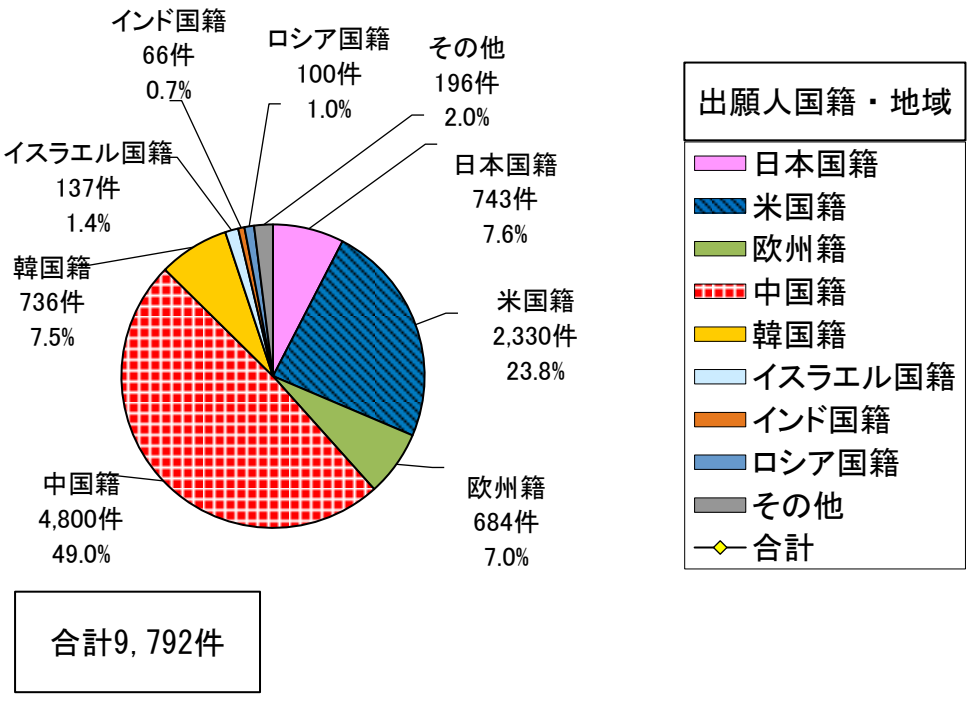
出願人国籍・地域	日本国籍	米国籍	欧州籍	中国籍	韓国籍	イスラエル国籍
全出願数	2,494	9,069	3,039	10,298	2,075	535
自国出願数	1,137	5,730	845	9,562	1,350	31
自国出願比率	46%	63%	28%	93%	65%	6%

表 4-4-2　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率（脅威インテリジェンス）

パテントファミリー件数	優先権主張年							合計	比率
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023		
合計	1,303	1,338	1,210	1,309	1,612	1,468	1,552	9,792	100.0%
日本国籍	135	162	104	85	81	105	71	743	7.6%
米国籍	500	396	310	283	288	273	280	2,330	23.8%
欧州籍	83	109	73	85	110	124	100	684	7.0%
中国籍	410	518	555	639	960	788	930	4,800	49.0%
韓国籍	93	90	104	130	108	111	100	736	7.5%
イスラエル国籍	33	13	22	24	17	18	10	137	1.4%
インド国籍	3	3	2	7	7	8	36	66	0.7%
ロシア国籍	21	23	15	18	7	10	6	100	1.0%
その他	25	24	25	38	34	31	19	196	2.0%
日本国籍の全件数に対する比率	10.4%	12.1%	8.6%	6.5%	5.0%	7.2%	4.6%	7.6%	

図 4-4-1 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率（脅威インテリジェンス）





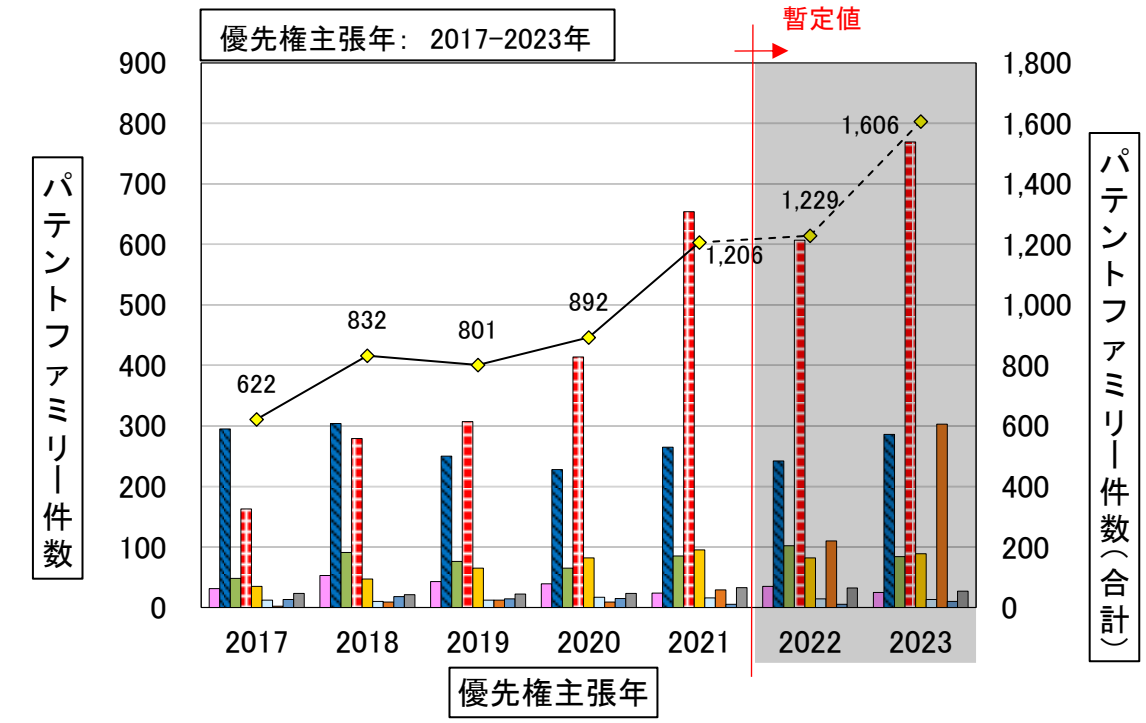
合計9,792件

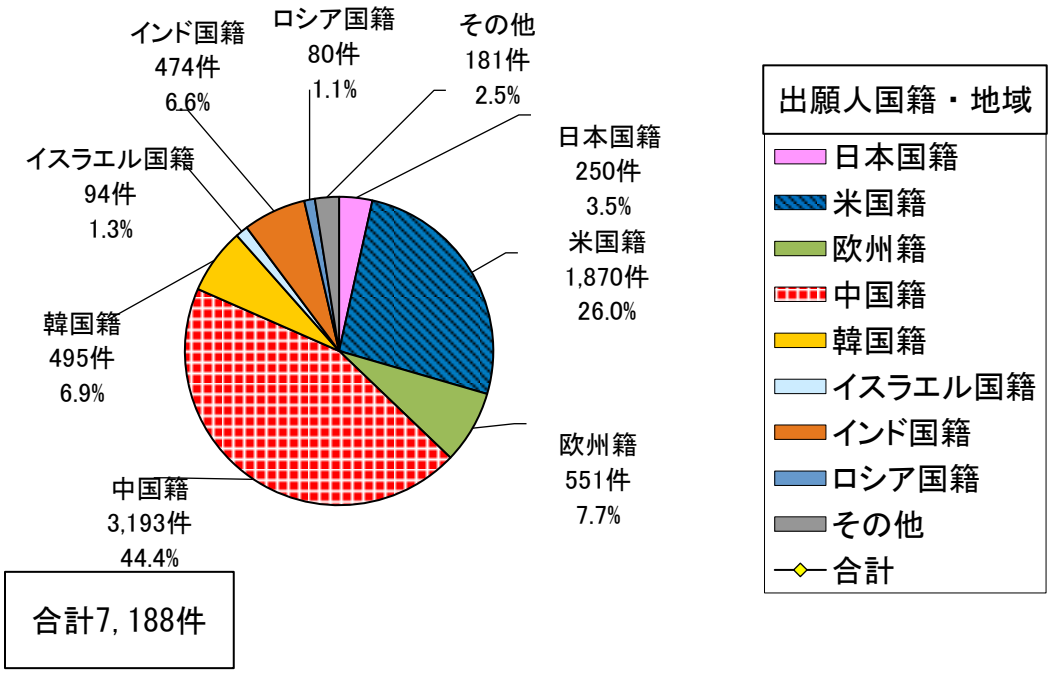
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

表 4-4-3 ［出願先：日米欧中韓以印露 WO］［技術区分別］パテントファミリー件数上位出願人ランキング（脅威インテリジェンス）

順位	出願人名称	ファミリー件数
1	北京安天网络安全技术有限公司（中国）	208
2	マイクロソフト株式会社（米国）	177
3	IBM株式会社（米国）	166
4	サングフォーテクノロジズ株式会社（中国）	157
5	テンセント合同会社（中国）	152
6	国家電網公司（中国）	131
7	DBAPPセキュリティ（中国）	126
8	トップセック・テクノロジーズ株式会社（中国）	119
9	パロアルトネットワークス株式会社（米国）	114
10	チー・アン・シン・テクノロジー株式会社（中国）	105
11	インテル株式会社（米国）	100
12	NTT株式会社	99
12	SUZHOU INSPUR INTELLIGENT TECHNOLOGY（中国）	99
14	QIZHI SOFTWARE BEIJING（中国）	97
15	日本電気株式会社	94
16	広東電網（中国）	83
17	華為技術株式会社（中国）	82
18	ヒューレット・パッカード合同会社（米国）	78
19	デル・テクノロジーズ株式会社（米国）	75
20	シスコシステムズ合同会社（米国）	74

図 4-4-2 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率（AI を利用した検知判定手法）





注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

表 4-4-4 ［出願先：日米欧中韓以印露 WO］特定産業向けサイバー攻撃検知技術のパテントファミリー件数（日本国籍の順位・出願比率）

産業分野	物流	電力	鉄道	石油	政府・行政サービス	水道	情報通信	航空	港湾	空港
順位(日本国籍)	3	3	3	5	4	3	3	5	6	4
出願比率(日本国籍)	9.5%	7.3%	18.5%	5.7%	6.8%	17.6%	11.0%	3.6%	0.0%	5.6%

産業分野	金融	化学	医療	クレジット	ガス	製造	車両	交通システム	教育	学術研究
順位(日本国籍)	5	3	6	4	3	3	1	3	5	4
出願比率(日本国籍)	3.7%	11.3%	4.8%	7.1%	16.4%	19.0%	26.8%	15.4%	2.6%	5.0%

表 4-4-5 ［出願先：日米欧中韓以印露 WO］パテントファミリー件数上位出願人ランキング（車両向け）

順位	出願人名称	ファミリー件数	共願率※
1	パナソニック株式会社	82	0.0%
2	ボッシュ株式会社（ドイツ）	79	1.3%
3	株式会社デンソー	45	0.0%
4	三菱電機株式会社	25	0.0%
5	インテル株式会社（米国）	24	0.0%
6	NTT株式会社	19	0.0%
7	ASTEMO株式会社	18	0.0%
7	現代自動車株式会社（韓国）	18	11.1%
7	AURORA LABS LTD（イスラエル）	18	0.0%
10	トヨタ自動車株式会社	17	0.0%
11	住友電気工業株式会社	16	0.0%
11	華為技術株式会社（中国）	16	0.0%
13	ELEKTROBIT AUTOMOTIVE GMBH（ドイツ）	12	0.0%
14	株式会社日立製作所	11	0.0%
14	マイクロンテクノロジー株式会社（米国）	11	0.0%
14	NXP BV（オランダ）	11	0.0%
14	HARMAN INT IND（米国）	11	0.0%
18	ブラックベリー株式会社（カナダ）	10	0.0%
19	アウディ株式会社（ドイツ）	9	0.0%
19	UNIV ZHEJIANG TECHNOLOGY（中国）	9	0.0%
19	クアルコム株式会社（米国）	9	0.0%
19	GEヘルスケア株式会社（米国）	9	0.0%
19	KARAMBA SECURITY LTD（イスラエル）	9	0.0%

表 4-4-6 ［出願先：日米欧中韓以印露 WO］パテントファミリー件数上位出願人ランキング（製造装置向け）

順位	出願人名称	ファミリー件数
1	シーメンスAG（ドイツ）	60
2	株式会社日立製作所	23
2	三菱電機株式会社	23
4	ボッシュ株式会社（ドイツ）	22
5	オムロン株式会社	19
6	国家電網公司（中国）	15
7	株式会社東芝	14
7	日本電気株式会社	14
9	ハネウェル合同会社（米国）	13
9	GEヘルスケア株式会社（米国）	13
11	NANOTRONICS IMAGING INC（米国）	12
12	パナソニック株式会社	11
13	ROCKWELL COLLINS INC（米国）	10
14	ファナック株式会社	8
14	NTT株式会社	8
16	NOZOMI NETWORKS SAGL（スイス）	7
16	ABB SCHWEIZ AG（スイス）	7
16	IBM株式会社（米国）	7
19	HUANENG WEIHAI POWER GENERATION CO LTD（中国）	6
19	UNIV BEIJING TECHNOLOGY（中国）	6
19	UNIV ZHEJIANG（中国）	6
19	STRONG FORCE VCN PORTFOLIO 2019 LLC（米国）	6

表 4-4-7 ［出願先：日米欧中韓以印露 WO］[出願人国籍・地域別］パテントファミリー件数比率の年次推移（車両）

件数比率	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	26.7%	35.1%	25.2%	26.1%	23.1%	30.5%	21.1%	26.8%
米国籍	25.7%	27.2%	25.2%	23.5%	17.7%	10.8%	11.6%	19.6%
欧州籍	19.8%	15.9%	14.4%	19.3%	22.6%	15.0%	19.7%	18.1%
中国籍	3.0%	7.3%	10.1%	16.8%	24.7%	30.5%	31.3%	18.9%
韓国籍	3.0%	2.6%	4.3%	11.8%	8.6%	7.8%	7.5%	6.6%
イスラエル国籍	18.8%	5.3%	15.1%	1.7%	1.1%	0.6%	2.7%	5.6%
インド国籍	1.0%	0.7%	0.7%	0.0%	0.5%	3.6%	4.8%	1.7%
ロシア国籍	0.0%	2.0%	1.4%	0.0%	0.0%	0.0%	0.0%	0.5%
その他	2.0%	4.0%	3.6%	0.8%	1.6%	1.2%	1.4%	2.1%

表 4-4-8 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（製造装置）

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	31.4%	27.6%	26.5%	13.6%	15.8%	13.3%	9.1%	18.9%
米国籍	20.9%	32.4%	18.8%	28.2%	15.8%	14.2%	15.7%	20.4%
欧州籍	25.6%	13.3%	18.8%	9.1%	15.8%	20.0%	14.0%	16.4%
中国籍	15.1%	15.2%	18.8%	30.9%	43.8%	46.7%	53.7%	33.5%
韓国籍	2.3%	4.8%	4.3%	10.9%	4.1%	2.5%	1.7%	4.3%
イスラエル国籍	1.2%	1.9%	5.1%	1.8%	2.7%	0.0%	0.0%	1.9%
インド国籍	0.0%	1.9%	0.0%	0.9%	0.7%	1.7%	4.1%	1.4%
ロシア国籍	0.0%	0.0%	4.3%	0.9%	0.0%	0.0%	0.0%	0.7%
その他	3.5%	2.9%	3.4%	3.6%	1.4%	1.7%	1.7%	2.5%

表 4-4-9 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（情報通信）

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	14.7%	14.5%	10.4%	8.7%	9.5%	12.9%	6.4%	11.0%
米国籍	33.5%	30.0%	24.3%	18.9%	15.2%	11.3%	13.5%	20.7%
欧州籍	12.4%	11.6%	12.4%	8.2%	8.3%	10.8%	6.4%	10.0%
中国籍	30.0%	34.8%	41.1%	47.4%	55.3%	54.3%	59.1%	46.3%
韓国籍	6.5%	4.3%	7.9%	14.3%	8.0%	8.6%	7.0%	8.1%
イスラエル国籍	0.6%	1.0%	0.5%	0.0%	0.8%	0.0%	0.0%	0.4%
インド国籍	0.6%	1.0%	0.5%	0.5%	0.8%	0.5%	5.3%	1.2%
ロシア国籍	1.2%	1.0%	1.0%	0.0%	0.4%	0.0%	0.0%	0.5%
その他	0.6%	1.9%	2.0%	2.0%	1.9%	1.6%	2.3%	1.8%

表 4-4-10 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（電力）

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	20.0%	7.6%	7.2%	4.2%	7.8%	6.7%	4.3%	7.3%
米国籍	35.0%	34.8%	26.1%	13.9%	12.6%	7.8%	3.2%	16.5%
欧州籍	5.0%	10.6%	7.2%	1.4%	6.8%	2.2%	5.3%	5.4%
中国籍	22.5%	36.4%	52.2%	62.5%	68.0%	77.8%	75.5%	60.9%
韓国籍	5.0%	7.6%	4.3%	11.1%	2.9%	4.4%	5.3%	5.6%
イスラエル国籍	2.5%	0.0%	0.0%	0.0%	1.9%	0.0%	1.1%	0.7%
インド国籍	2.5%	0.0%	0.0%	1.4%	0.0%	1.1%	5.3%	1.5%
ロシア国籍	0.0%	0.0%	1.4%	0.0%	0.0%	0.0%	0.0%	0.2%
その他	7.5%	3.0%	1.4%	5.6%	0.0%	0.0%	0.0%	1.9%

表 4-4-11 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（医療）

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	3.8%	8.0%	3.0%	2.4%	7.0%	4.3%	3.8%	4.8%
米国籍	57.7%	58.0%	51.5%	39.0%	27.9%	26.1%	28.3%	40.9%
欧州籍	15.4%	14.0%	21.2%	2.4%	16.3%	4.3%	5.7%	11.2%
中国籍	15.4%	6.0%	12.1%	26.8%	41.9%	52.2%	39.6%	27.1%
韓国籍	3.8%	6.0%	3.0%	9.8%	7.0%	0.0%	7.5%	5.9%
イスラエル国籍	0.0%	6.0%	3.0%	7.3%	0.0%	0.0%	1.9%	3.0%
インド国籍	3.8%	0.0%	3.0%	12.2%	0.0%	13.0%	11.3%	5.9%
ロシア国籍	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
その他	0.0%	2.0%	3.0%	0.0%	0.0%	0.0%	1.9%	1.1%

表 4-4-12 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（金融）

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	2.1%	4.6%	3.0%	5.8%	6.3%	2.9%	1.9%	3.7%
米国籍	44.7%	58.3%	48.0%	29.1%	27.3%	25.5%	21.0%	35.0%
欧州籍	9.6%	9.3%	7.0%	7.0%	4.7%	7.8%	2.5%	6.4%
中国籍	34.0%	23.1%	30.0%	50.0%	54.7%	54.9%	62.3%	45.8%
韓国籍	3.2%	1.9%	7.0%	2.3%	3.1%	7.8%	4.9%	4.4%
イスラエル国籍	3.2%	0.9%	0.0%	0.0%	0.0%	0.0%	1.2%	0.8%
インド国籍	0.0%	0.0%	0.0%	1.2%	0.8%	1.0%	3.1%	1.0%
ロシア国籍	3.2%	1.9%	2.0%	3.5%	0.0%	0.0%	1.2%	1.5%
その他	0.0%	0.0%	3.0%	1.2%	3.1%	0.0%	1.9%	1.4%

第５章　研究開発動向調査

第５章では、サイバー攻撃検知技術に関する研究開発動向調査の結果を示す。

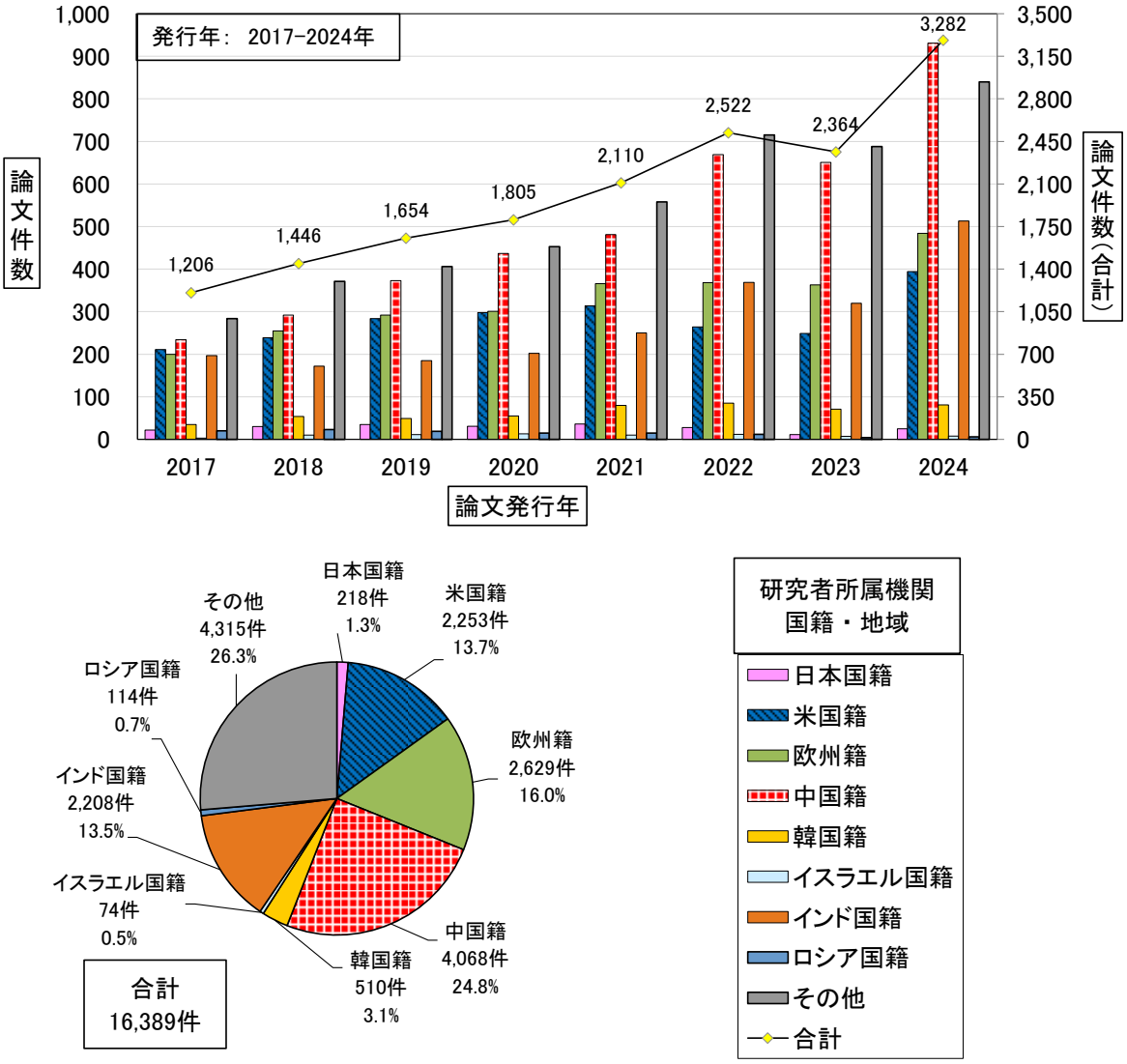
第５章の要約

- 調査対象国におけるサイバー攻撃検知技術に関する論文発表件数は、調査期間の2017年から2024年の間、全体としては増加傾向が認められた。2024年には2017年の3倍近い3,282件に増加している。【図 5-1-1】
- 研究者所属機関の国籍・地域別の論文発表件数は、中国籍(世界シェア24.8%)が最も多く、次いで欧州籍(16.0%)、米国籍(13.7%)、インド国籍(13.5%)、韓国籍(3.1%)、日本国籍(1.3%)の順となっている。【図 5-1-1】
- 特許出願のパテントファミリー件数では、中国籍や米国籍の出願人が目立つが、論文発表件数では、欧州籍が中国籍に次いで2位であり、3位の米国籍よりも存在感を示している。件数の推移に着目すると、中国籍やインド国籍の論文発表件数が大幅に増加している一方、米国籍の論文発表件数は減少傾向である。【図 5-1-1】
- 侵入／異常検知やウイルス／マルウェア検知にAIを利用した検知・判定手法の論文発表件数は、全体としては増加傾向が認められた。【図 5-2-1】
- 研究者所属機関の国籍・地域別の侵入／異常検知やウイルス／マルウェア検知にAIを利用した検知・判定手法の論文発表件数比率は、中国籍が最も高く、次いでインド国籍、欧州籍、米国籍、韓国籍、日本国籍の順となっている。論文全体と比べるとインド国籍の割合が大きいのが特徴である。【図 5-4-1】
- サイバー攻撃検知技術の全論文に対するAIを利用した検知手法の論文の比率は、ほぼどの国籍・地域も50%を超えており、AIを利用した検知が一般的になってきたといえる。【表 5-4-1】
- サイバー攻撃検知技術のための脅威情報の収集等、脅威インテリジェンスに関連する(小区分：脅威情報・脆弱性情報、又は中区分：脅威インテリジェンス)論文発表件数は、全体としては増加傾向が認められた。【図 5-4-2】
- 研究者所属機関の国籍・地域別の脅威インテリジェンスに関連する論文発表件数比率は、中国籍が最も多く、次いで欧州籍、インド国籍、米国籍、韓国籍、日本国籍の順となっている。【図 5-4-2】
- 研究者所属機関の国籍・地域別の車両分野向けサイバー攻撃検知技術の論文発表件数比率は、中国籍が最も多く、次いで欧州籍、米国籍、韓国籍、インド国籍、日本国籍の順となっている。【図 5-4-3】
- 研究者所属機関の国籍・地域別の製造装置分野向けサイバー攻撃検知技術の論文発表件数比率は、車両向けと同じく中国籍が最も多く、次いで欧州籍、米国籍、インド国籍、韓国籍、日本国籍の順となっている。【図 5-4-4】
- 論文発表件数上位20者の所属機関国籍は、中国籍(11者)とインド国籍(4者)で3/4を占めている(表 5-3-1)。インド国籍の機関は調査期間の前半(2017年から2020年)では10位以内に1者しか入っていないが、後半(2021年から2024年)では10位以内に4者が入っている。【表 5-3-1】【表 5-3-2】

第１節　全体動向調査

本節では、研究開発動向調査のうち全体動向調査の結果を示す。研究者所属機関国籍・地域等を基に分析している。

図 5-1-1　［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率



※その他上位国籍・地域：カナダ(495)、サウジアラビア(468)、オーストラリア(355)、パキスタン(305)、トルコ(286)。

第２節　技術区分別動向調査

本節では、研究開発動向調査のうち技術区分別全体動向調査の結果を示す。研究者所属機関国籍・地域等を基に分析している。

図 5-2-1　［技術区分別］論文発表件数年次推移（AI 利用）

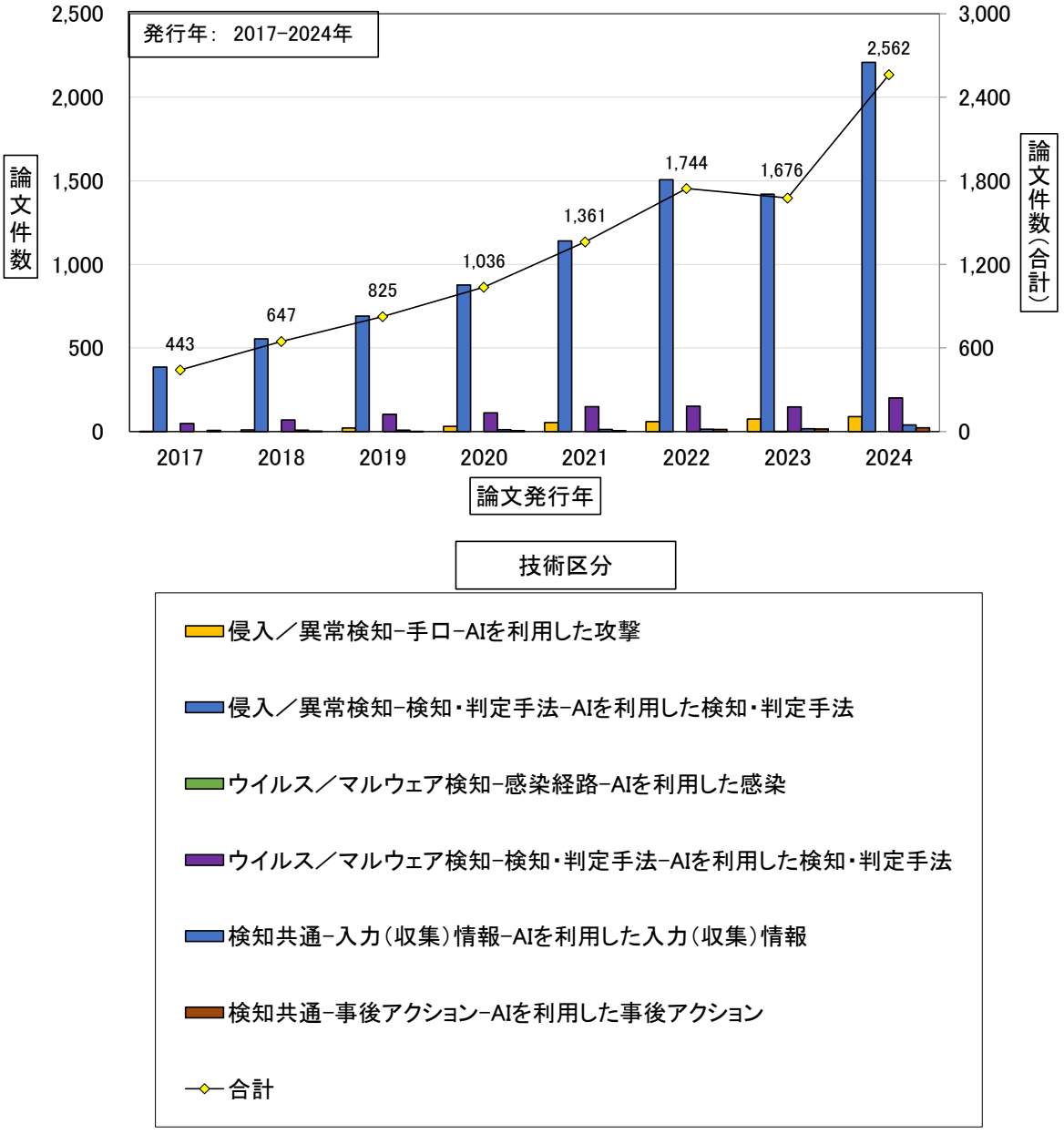


図 5-2-2 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数（大区分：侵入／異常検知）

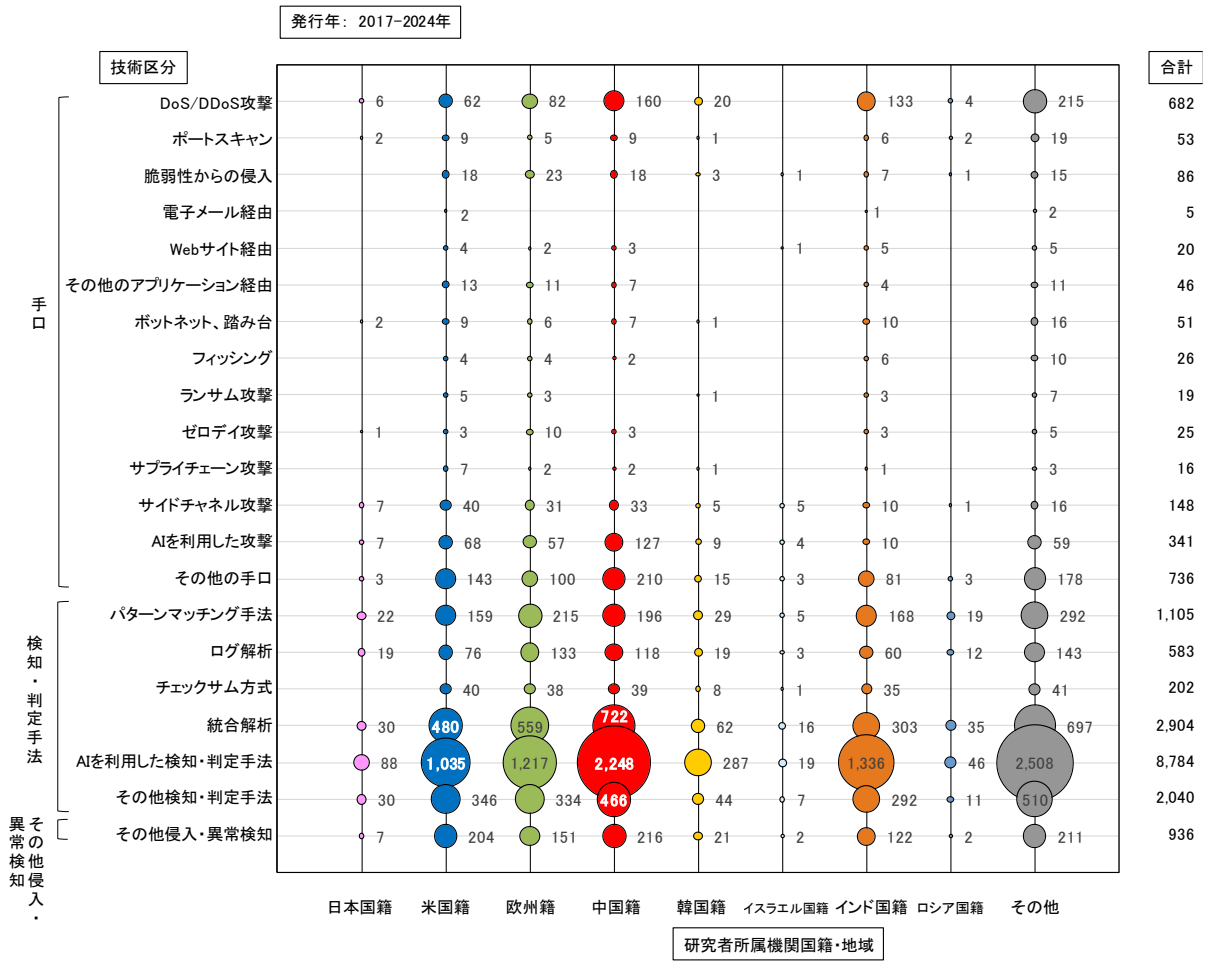


図 5-2-3 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数（大区分：ウイルス／マルウェア検知）

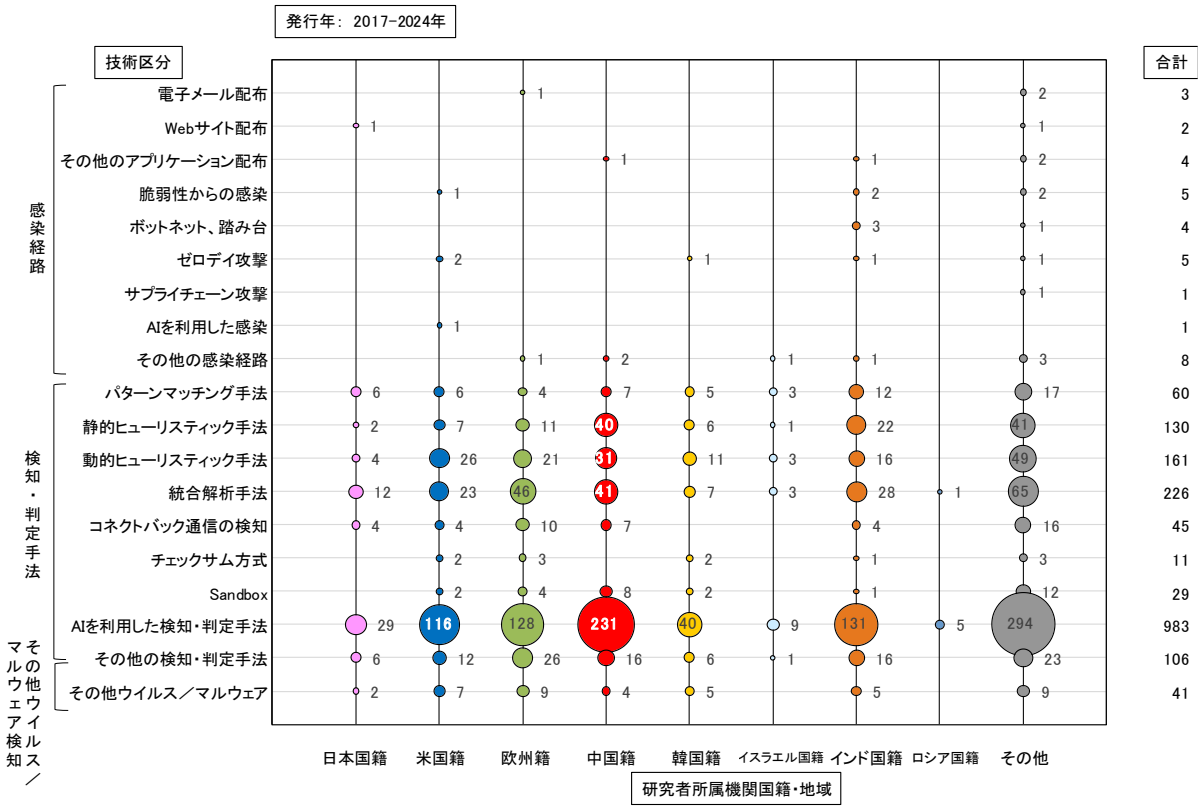


図 5-2-4 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数（大区分：検知共通、その他（検知））

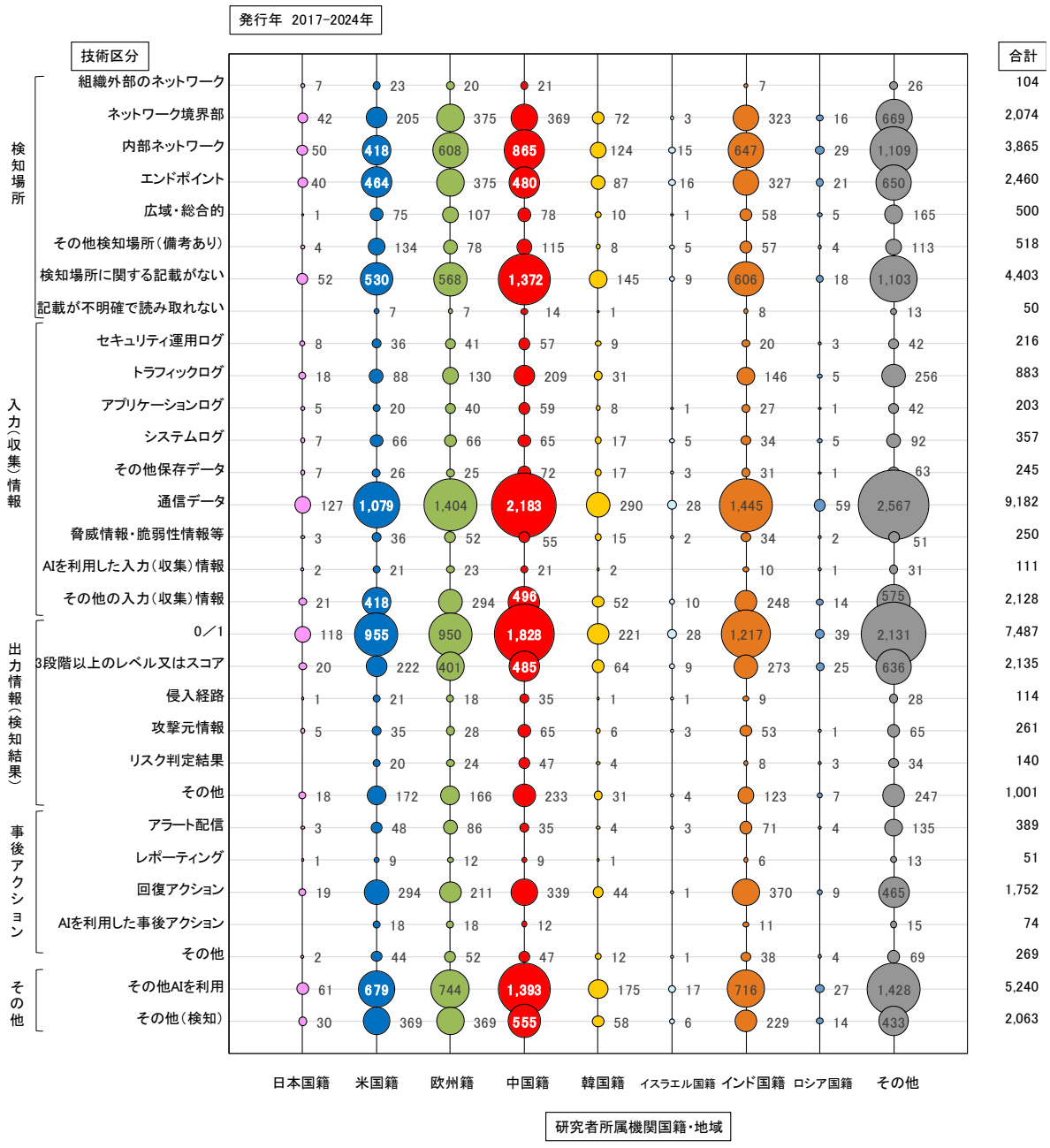


図 5-2-5 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数（大区分：適用領域（産業等）、解決課題／効果、AI に対する攻撃対策、脅威インテリジェンス）

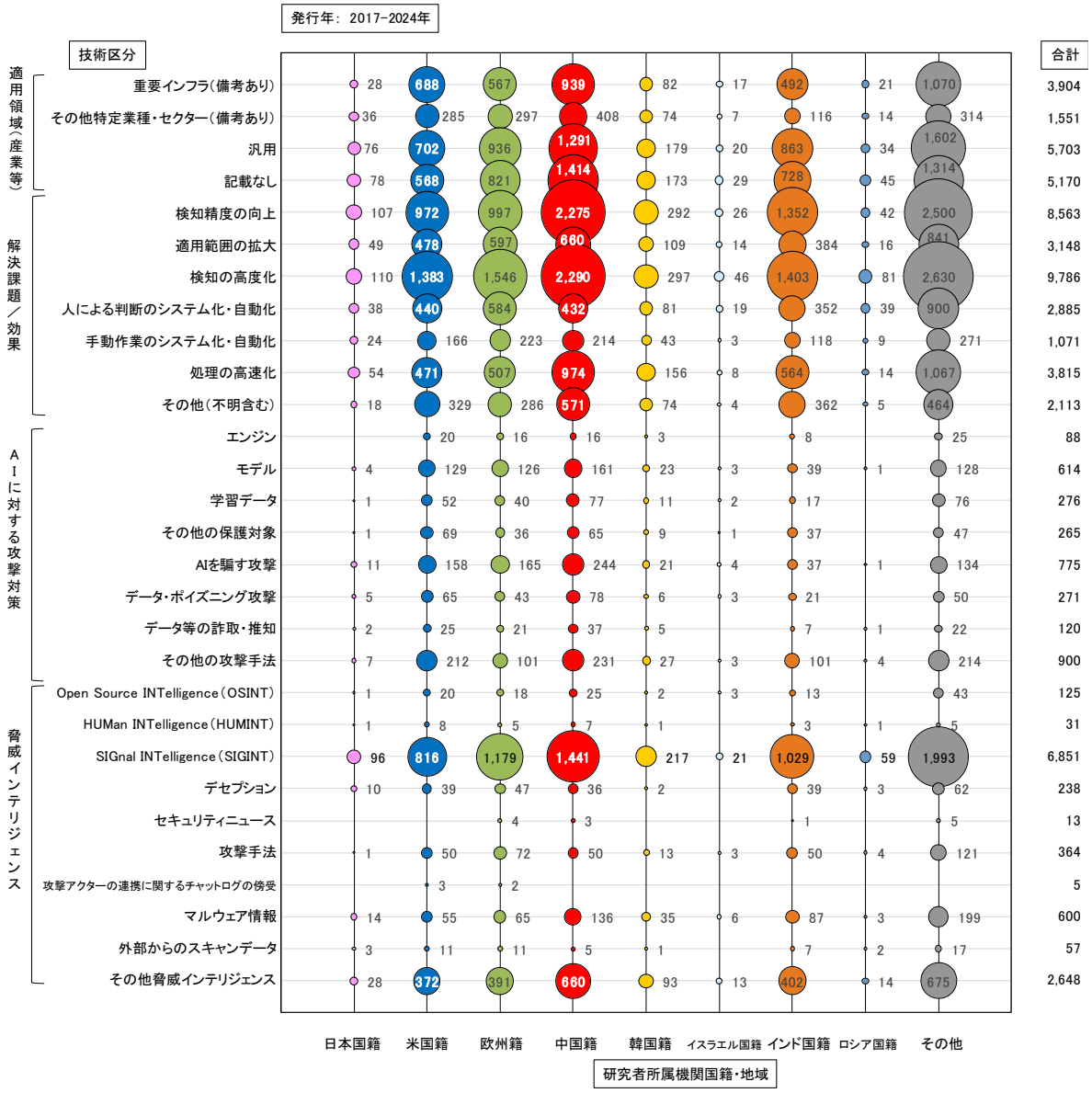
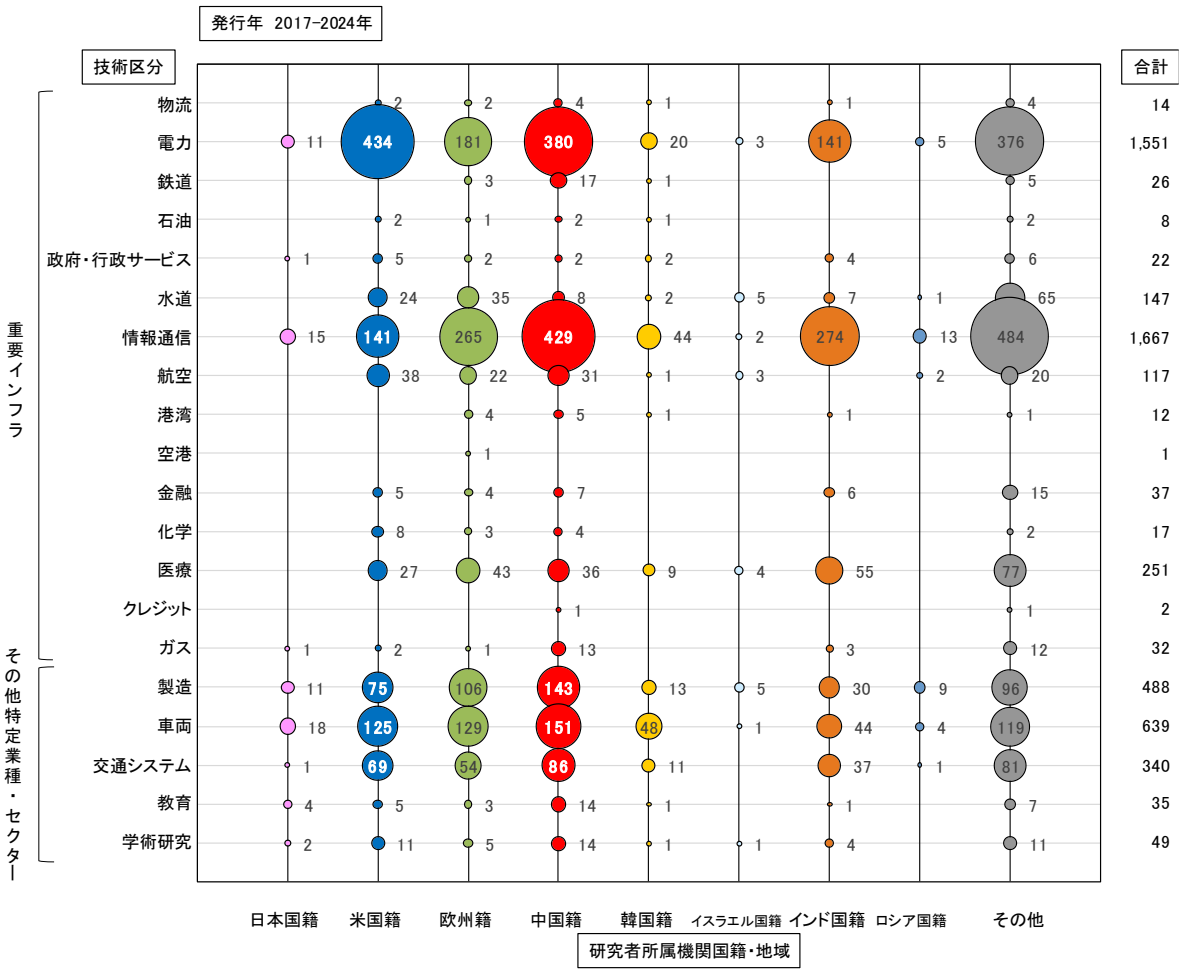


図 5-2-6 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数（重要インフラ、その他特定業種・セクター）



第３節　研究者所属機関・研究者別動向調査

本節では、研究開発動向調査のうち研究者所属機関・研究者別動向調査の結果を示す。研究者所属機関国籍・地域等を基に分析している。

表 5-3-1　論文発表件数上位研究者所属機関ランキング

順位	研究者所属機関名称	件数
1	CHINESE ACAD SCI（中国）	168
2	NATL INST TECHNOL（インド）	160
3	BEIJING UNIV POSTS & TELECOMMUN（中国）	129
4	INDIAN INST TECHNOL（インド）	109
5	NORTHEASTERN UNIV（中国）	96
6	UNIV ELECT SCI & TECHNOL CHINA（中国）	93
7	ZHEJIANG UNIV（中国）	80
8	UNIV CALIF（米国）	76
8	VELLORE INST TECHNOL（インド）	76
10	SRM INST SCI & TECHNOL（インド）	71
11	CONCORDIA UNIV（カナダ）	70
12	NATL UNIV DEF TECHNOL（中国）	69
13	TEXAS A&M UNIV（米国）	66
13	SOUTHEAST UNIV（中国）	66
15	KING ABDULAZIZ UNIV（サウジアラビア）	65
16	UNIV TEXAS（米国）	64
17	XIDIAN UNIV（中国）	62
18	SHANGHAI JIAO TONG UNIV（中国）	61
19	BEIJING INST TECHNOL（中国）	60
20	BEIHANG UNIV（中国）	59

表 5-3-2　論文発表件数上位研究者所属機関ランキング推移（公開年範囲別）

公開年：2017-2020年			公開年：2021～2024年		
順位	研究者所属機関名称	件数	順位	研究者所属機関名称	件数
1	NATL INST TECHNOL（インド）	66	1	CHINESE ACAD SCI（中国）	112
2	BEIJING UNIV POSTS & TELECOMMUN（中国）	64	2	NATL INST TECHNOL（インド）	94
3	CHINESE ACAD SCI（中国）	56	3	INDIAN INST TECHNOL（インド）	80
4	UNIV CALIF（米国）	36	4	BEIJING UNIV POSTS & TELECOMMUN（中国）	65
4	NATL UNIV DEF TECHNOL（中国）	36	4	SRM INST SCI & TECHNOL（インド）	65
6	XIDIAN UNIV（中国）	35	4	VELLORE INST TECHNOL（インド）	65
7	SINGAPORE UNIV TECHNOL & DESIGN（シンガポール）	32	7	NORTHEASTERN UNIV（中国）	64
7	NORTHEASTERN UNIV（中国）	32	8	UNIV ELECT SCI & TECHNOL CHINA（中国）	63
9	UNIV NEW SOUTH WALES（オーストラリア）	30	9	KING ABDULAZIZ UNIV（サウジアラビア）	53
9	ZHEJIANG UNIV（中国）	30	10	ZHEJIANG UNIV（中国）	50

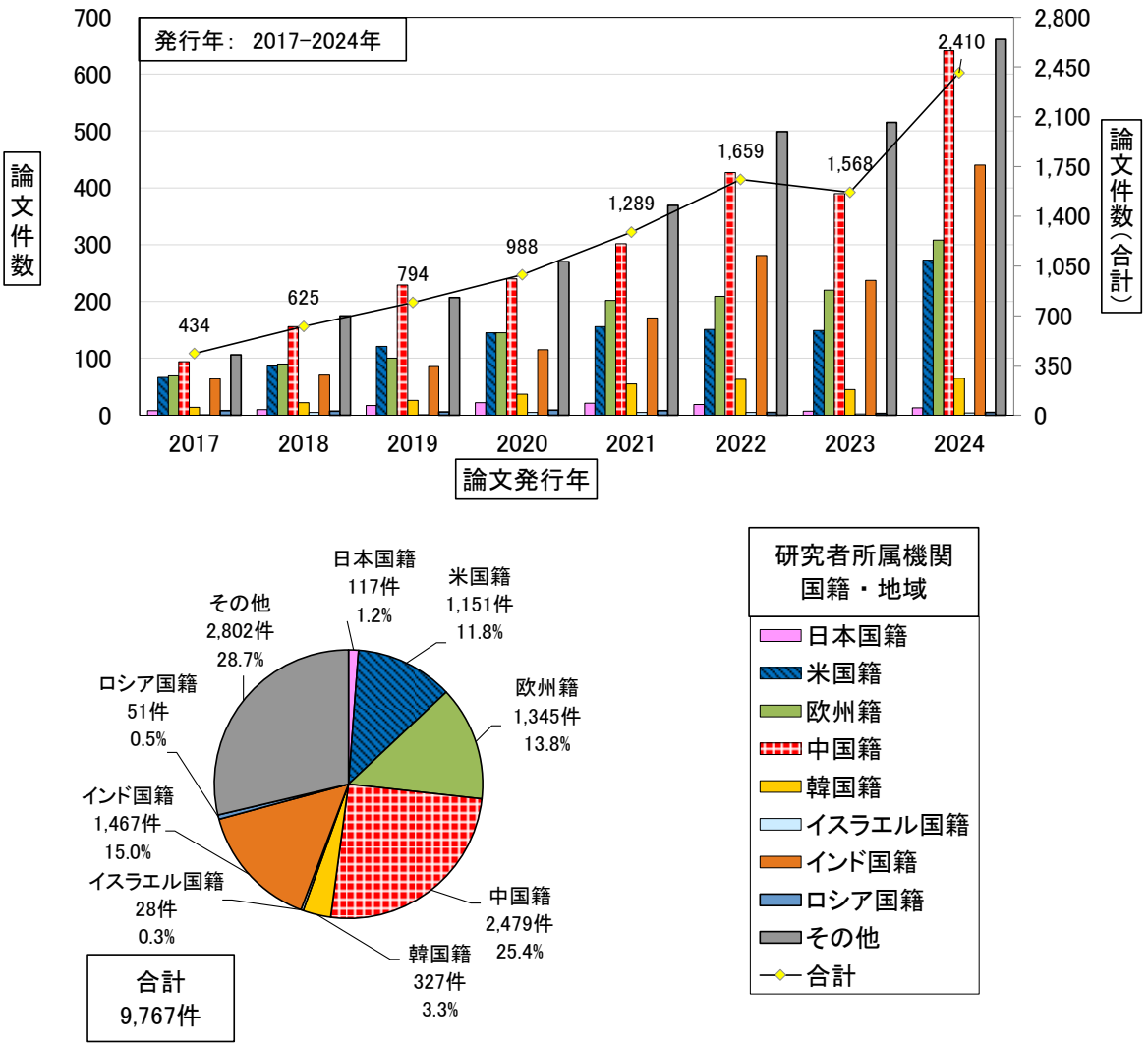
表 5-3-3　論文発表件数上位研究者ランキング

順位	著者名 @所属（同姓同名を避けるため所属を付加）	件数
1	Moustafa, Nour @UNIV NEW SOUTH WALES（オーストラリア）	12
2	Tang, Dan @HUNAN UNIV（中国）	10
2	Li, Wenjuan @GUANGZHOU UNIV（中国）	10
2	Catillo, Marta @UNIV SANNIO（イタリア）	10
5	Li, Wenjuan @CITY UNIV HONG KONG（中国）	9
5	Wang, Zhendong @JIANGXI UNIV SCI & TECHNOL（中国）	9
5	Chiba, Zouhair @HASSAN II UNIV（モロッコ）	9
8	Conti, Mauro @UNIV PADUA（イタリア）	8
8	Thakkar, Ankit @NIRMA UNIV（インド）	8
8	Wu, Zhijun @CIVIL AVIAT UNIV CHINA（中国）	8
8	Lopez-Martin, Manuel @UNIV VALLADOLID（スペイン）	8
8	Gupta, Brij B. @ASIA UNIV（台湾）	8
13	Shahin, Mohammad @UNIV TEXAS（米国）	7
13	Ferrag, Mohamed Amine @GUELMA UNIV（アルジェリア）	7
13	Rustam, Furqan @UNIV COLL DUBLIN（アイルランド）	7
13	Rathore, Hemant @BITS PILANI（インド）	7
13	Wan, Ming @LIAONING UNIV（中国）	7
13	Basan, Elena @SOUTHERN FED UNIV（ロシア）	7
13	Kim, Taehoon @YEUNGNAM UNIV（韓国）	7
13	Andresini, Giuseppina @UNIV BARI（イタリア）	7

第４節　総合分析に関連する調査

本節では、研究開発動向調査のうち総合分析に関連する調査結果を示す。本調査では、第１節から第３節までの調査以外に総合分析のために追加で調査した図表を図示した。

図 5-4-1　［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率
（侵入／異常検知・ウイルス／マルウェア検知に AI を利用した検知・判定手法）

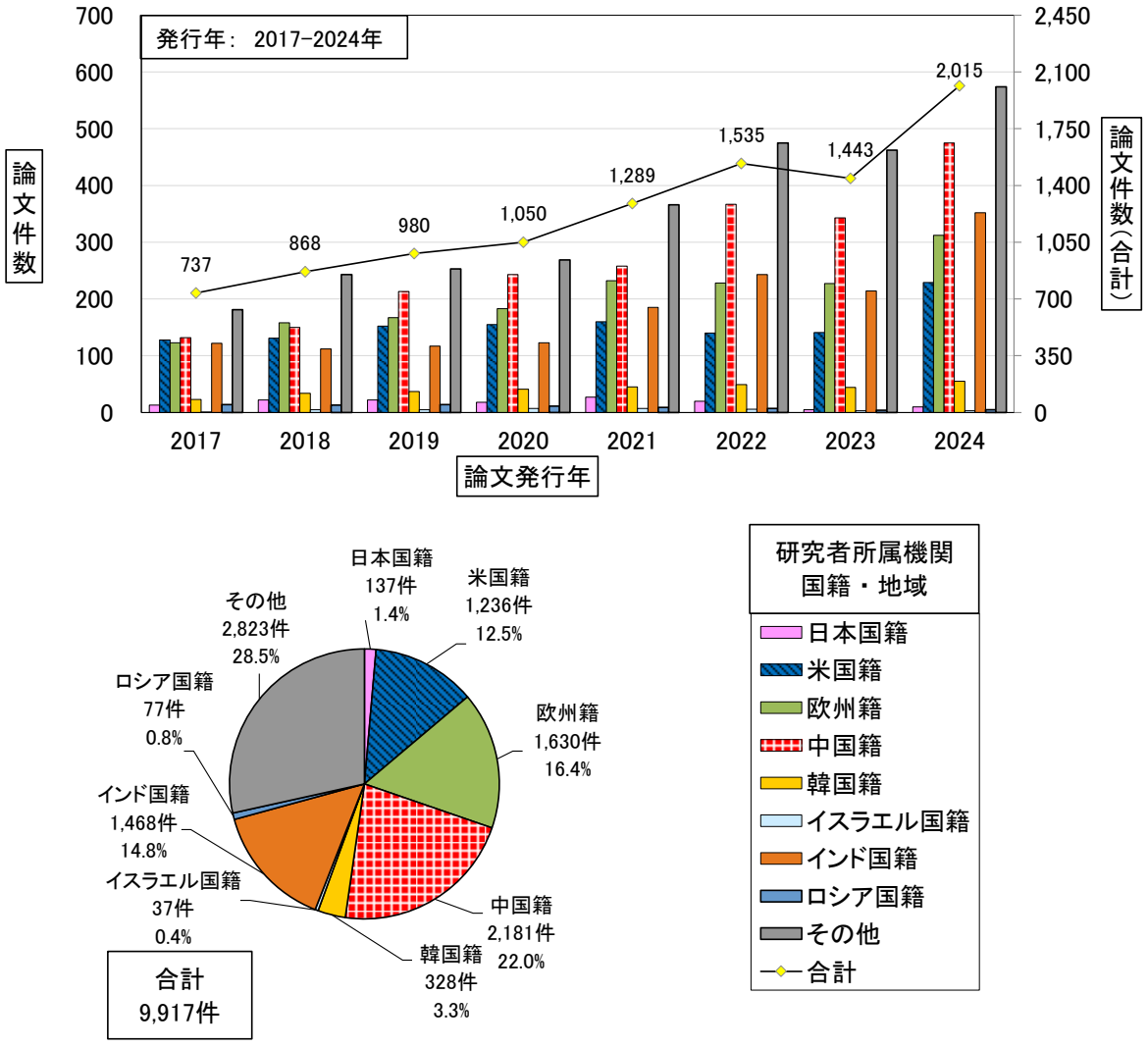


※その他上位国籍・地域：サウジアラビア(382)、カナダ(300)、オーストラリア(223)、トルコ(218)、パキスタン(214)。

表 5-4-1 ［研究者所属機関国籍・地域別］全論文発表件数に対する AI を利用した検知・判定手法の論文発表件数比率

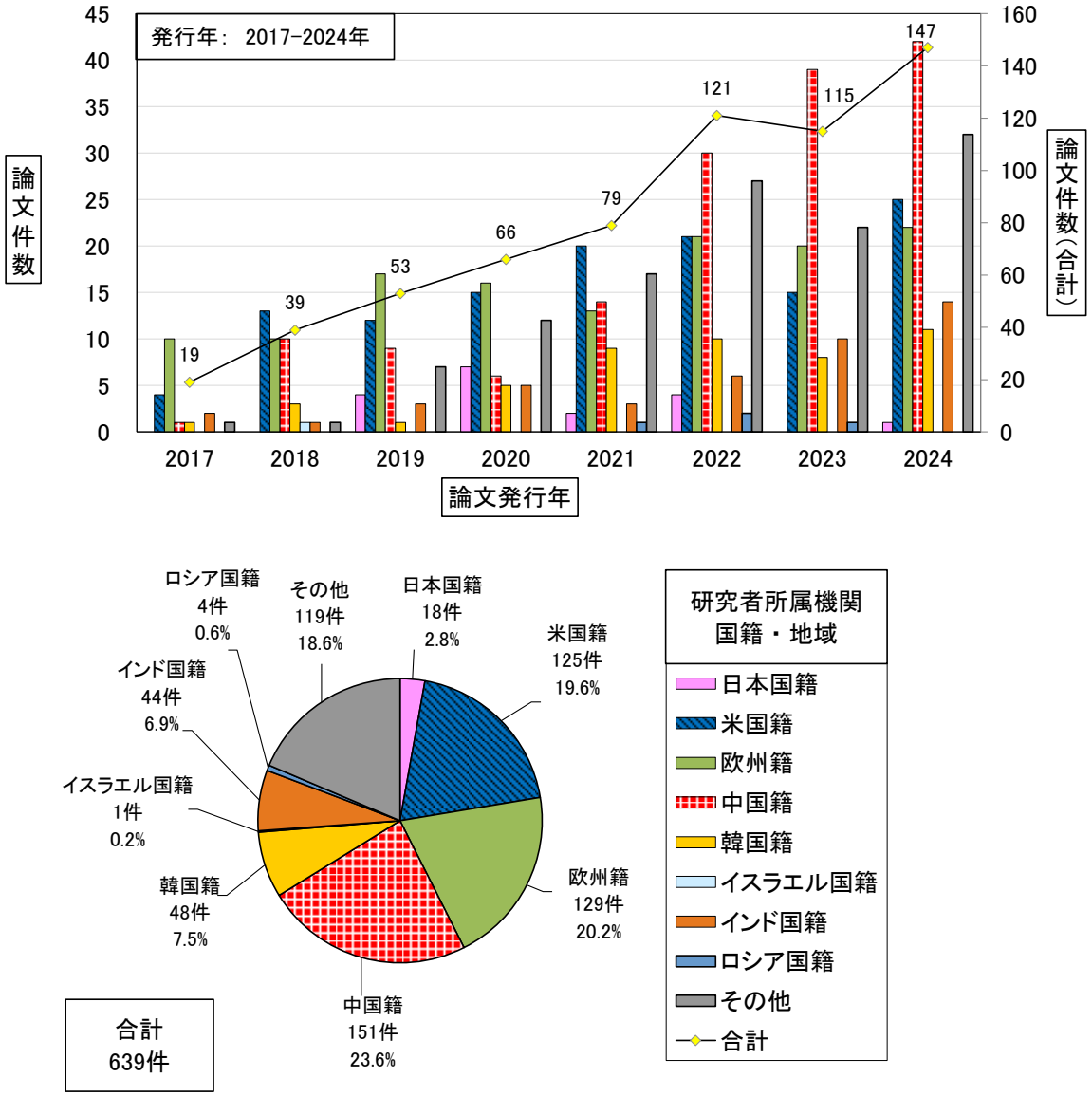
出願人国籍・地域	日本国籍	米国籍	欧州籍	中国籍	韓国籍	イスラエル国籍	インド国籍	ロシア国籍	その他
侵入／異常検知	52%	53%	56%	64%	68%	37%	69%	48%	68%
ウイルス／マルウェア検知	66%	75%	62%	81%	65%	60%	77%	83%	77%

図 5-4-2 ［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率（脅威インテリジェンス（小区分：脅威情報・脆弱性情報、中区分：脅威インテリジェンス））



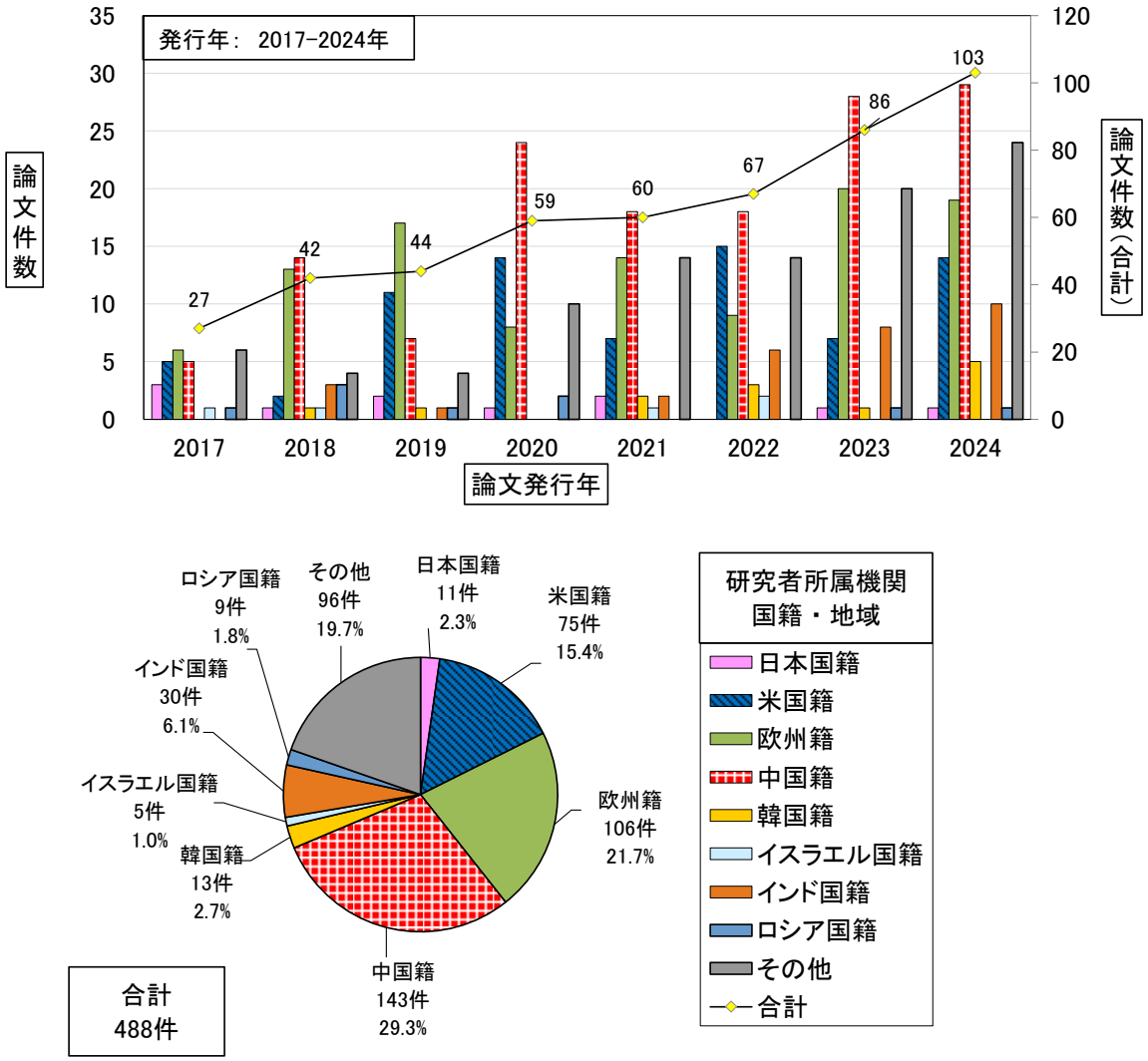
※その他上位国籍・地域：サウジアラビア(340)、カナダ(290)、オーストラリア(235)、パキスタン(232)、トルコ(208)。

図 5-4-3 ［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率
（車両向け）



※その他上位国籍・地域：カナダ(23)、サウジアラビア(14)、パキスタン(12)、イラン(7)、シンガポール(6)、マレーシア(6)、オーストラリア(6)。

図 5-4-4 ［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率
（製造装置向け）



※その他上位国籍・地域：サウジアラビア(14)、台湾(9)、カナダ(8)、オーストラリア(8)、パキスタン(8)。

第６章　総合分析

第１節　調査内容の総括

本調査では、市場環境調査により、サイバーセキュリティ市場の規模、製品やサービスの概要とそれぞれの市場規模・市場シェア、主要な企業や製品の動向について把握した。また、政策動向調査により、日本のサイバーセキュリティ政策、サイバー安全保障政策、国内及び諸外国・地域のサイバー攻撃検知に関する助成施策、規格化・標準化の動向、規制の動向について把握した。さらに、特許動向調査及び研究開発動向調査により、サイバー攻撃検知技術(不正侵入・マルウェア等の検知に向けた情報セキュリティ技術)の国内外の技術発展状況及び研究開発状況を含む技術動向について把握した。

これらの調査結果を前提として、日本企業・政府機関が取り組むべき課題と目指すべき方向性を検討し、第６章第２節の示唆へとつながる事項を中心に総括を行った。

１．　市場環境調査(第２章)の総括

世界のサイバーセキュリティ市場は拡大傾向にあり、2024 年の世界のサイバーセキュリティ市場規模は 1,937 億米ドルである(図 2-1-1)。製品・サービス別では、Managed Security Services(MSS)等を含むサービス市場が最大であり、2024 年の市場規模は 709 億米ドル、2032 年までに 2,430 億米ドルまで拡大する見込みである(表 2-1-2)。国別では、米国市場が最大であり、2024 年の市場規模は 657 億米ドル、2032 年までに 1,670 億米ドルまで拡大する見込みである(図 2-1-2)。

2024年の日本のサイバーセキュリティ市場規模は86億米ドルであり、2025年から2032年までの CAGR(年平均成長率)は 15.0%と推測されている(表 2-1-3)。また、日本国内の主要製品ごとの市場規模は、Firewall が 2023 年度で 552 億円、EDR が 2023 年度で 307 億円、SIEM が 2023 年度で 168 億円、XDR が 2023 年度で 37 億円となっている。この 4 つの製品の市場では、米国企業が市場規模の 68.6%を占めており、国外企業による寡占的な市場環境となっている(図 2-2-2)。

各セキュリティ製品に着目すると、クラウド環境の普及やサイバー攻撃の巧妙化・高度化等を社会的な背景として、主要企業は製品同士の統合や AI の活用を通じて検知性能の向上や脅威判定の自動化を進めている。具体的には、統合ログ管理ソリューションである SIEM は多様なセキュリティ製品と統合し、ログを蓄積、相関分析をすることにより、単一ログの分析では見えにくい攻撃兆候を明らかにする等、高精度な脅威分析を図っている。センサとして機能する EDR や NDR は XDR との連携が進められており、エンドポイントやネットワークからのログを多角的に分析した上で脅威を検知する動きが見られる。また、従来は人手で行われていた攻撃兆候の分析やインシデントレスポンスを、AI の活用によって自動化する機能の実装が進められており、セキュリティアナリストや SOC の業務負担軽減が図られている。

米国やイスラエルの主要ベンダは企業買収を行って競争力向上を図っている。また、主要企業は提携や買収を通じて収集できるテレメトリデータや IoC(Indicator of Compromise)等の脅威インテリジェンス情報の量を拡大するとともに、それらを調査・分析する専門家集団を自社独自で構築することで、他社と差別化を図っている。以上のことから、サイバーセキュリティ市場は世界・日本ともに拡大傾向であり、各セキュリティ製品は製品間連携や AI の活用により運用効率の向上が図られていることが明らかに

なった。一方、国内市場ではサイバーセキュリティ分野における国外ベンダへの依存に関する社会的・技術的課題が明らかとなった。

2． 政策動向調査(第３章)の総括

日本のサイバーセキュリティ政策は、サイバーセキュリティ基本法を根拠とする「サイバーセキュリティ戦略」と、国家の最上位の政策文書である「国家安全保障戦略」を基盤として推進されている。具体的には、高度な国家関与型攻撃やランサムウェア被害の深刻化を背景に、重要インフラ防護に向けた統一的な枠組みの整備や官民の情報共有体制の強化が進められるとともに、国際連携が推進されている。同時に、能動的サイバー防御の実現に向けたサイバー対処能力強化法及び同整備法が成立し、国家サイバー統括室を司令塔とする切れ目のない対処体制の構築が進められている。各府省庁に着目すると、内閣官房では GSOC システムの要素技術改善、総務省では NOTICE や NICTER による IoT・端末由来データの分析基盤整備、防衛省ではクラウド基盤整備等が進められている。また、国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)や国立研究開発法人情報通信研究機構(NICT)等による研究開発・実証の助成施策や、日本産業標準調査会(JISC)による標準化活動も実施されている。電気通信事業法等による規制、外国為替及び外国貿易法等の輸出入規制、エネルギーの使用の合理化等に関する法律等の環境規制の整備も進められている。

国外の動向として、米国では 2023 年に国家サイバーセキュリティ戦略(National Cybersecurity Strategy)を策定した。この戦略では、重要インフラ防衛、脅威行動主体への対抗、米国全体のレジリエンス向上、将来の安全保障基盤への投資、国際パートナーシップの構築の 5 つを戦略の柱として位置付け、米国全体のセキュリティ強化を図っている。欧州では 2020 年にデジタル 10 年に向けた EU サイバーセキュリティ戦略(The EU’s Cybersecurity Strategy for the Digital Decade)を策定した。この戦略では、レジリエンス強化と技術的主権の確保、予防・抑止・対応能力の構築、国際協力と開かれたサイバー空間の推進の 3 つを戦略の柱として位置付けている。中国では 2016 年にサイバースペースセキュリティ国家戦略(国家网络空间安全战略)が、韓国では 2024 年に国家サイバーセキュリティ戦略が、イスラエルでは 2024 年に国家サイバーセキュリティ戦略(2025-2028)が、それぞれ策定されている。

加えて、ISO や IEC、ITU、IETF をはじめとした国際的な標準化団体によって、ISO/IEC 27039:2015 や RFC 4766 等のサイバー攻撃検知に関する規格が策定されている。このような国際的な標準化の流れを受け、各国・地域では、国際標準との整合を図りつつ、国内標準化が進められている。

以上のことから、各国・地域では、サイバー攻撃検知を含むサイバーセキュリティに関する政策の策定が進められていると同時に、国際標準の採用や規制の整備が行われていることが明らかとなった。

3． 特許動向調査(第４章)の総括

ここでは第４章に掲載した図表を参照して総括を行う。

本調査の調査対象技術である、サイバー攻撃検知技術に関するパテントファミリー件数(調査期間：2017 年から 2023 年)は、2017 年から 2020 年まではほぼ横ばいで推移して

いたが、2021 年以降は増加傾向が認められた(図 4-1-1)。2017 年のパテントファミリー件数は 2,625 件だが、2021 年には 3,332 件になり、暫定値ではあるが 2023 年は 3,720 件に達している(図 4-1-1)。

出願人の国籍・地域別のパテントファミリー件数に注目すると、中国籍(世界シェア 45.7%)が最も多く、次いで米国籍(26.1%)、欧州籍(7.4%)、韓国籍(6.5%)、日本国籍(6.4%)、インド国籍(3.5%)の順となっている(図 4-1-1)。

中国籍の出願人によるパテントファミリー件数は、調査期間を通じておおむね増加傾向にあり、2021 年には 2017 年の 2 倍以上に達している。一方で米国籍の出願人によるパテントファミリー件数は減少傾向にあり、2017 年は米国籍が中国籍を上回っていたが、2019 年に逆転し、2021 年には中国籍が米国籍の 2 倍以上となっている。日本国籍、欧州籍、韓国籍の出願人によるパテントファミリー件数は、調査期間中大きな増減なく推移している。インド国籍の出願人によるパテントファミリー件数は、2017 年から 2021 年にかけて緩やかに増加していたが、2022 年以降急激に増加している。暫定値ではあるが、2023 年は中国、米国に次いでインドが調査国中 3 位となっている(図 4-1-1)。

日本国籍の出願人による出願先国を出願件数で比較すると、日本(1,137 件)、米国(789 件)、中国(253 件)、欧州(231 件)、韓国(21 件)の順となっている(図 4-1-2)。

出願人の自国出願比率を出願人の国籍・地域別に比較すると、日本国籍は 46%であるのに対し、米国籍(63%)、中国籍(93%)、韓国籍(65%)は、半数以上が自国に出願されている(表 4-4-1)。中国籍の出願人は、自国内での特許取得を重視していることが読み取れる。一方、欧州籍の自国出願比率は 28%、イスラエル国籍は 6%と共に低く、自国よりも国外での特許取得を重視しているといえる(表 4-4-1)。

次に、技術区分別特許出願動向の調査結果について述べる。侵入／異常検知技術のうち、DoS/DDoS 攻撃、電子メール経由、フィッシング、ランサム攻撃、サプライチェーン攻撃、サイドチャネル攻撃を手口とする侵入／異常の検知技術は、米国籍が首位であり、全体の件数では首位である中国籍よりも優位である。中国籍は、ポートスキャン及び脆弱性からの侵入で首位である。また、インド国籍は、ゼロデイ攻撃及び AI を利用した攻撃で首位である(図 4-2-1)。ウイルス／マルウェア検知技術のうち、電子メール配布、ボットネット／踏み台、ゼロデイ攻撃、サプライチェーン攻撃を感染経路とするウイルス／マルウェアの検知技術は、米国籍が首位である。中国籍は Web サイト配布及び脆弱性からの感染で首位であり、インド国籍は AI を利用した感染で首位である(図 4-2-2)。今後のインドの動向には注視が必要である。

特定の産業分野向けのサイバー攻撃検知技術については、電力分野で中国籍出願人のパテントファミリー件数が 325 件と最も多く、調査国中 2 位の米国籍出願人の 88 件を大きく上回っている。金融分野でも中国籍が 357 件で首位、米国籍が 273 件で続き、この 2 カ国が突出している。3 位の欧州籍は 50 件にとどまる(図 4-2-5)。

車両分野では日本国籍が 271 件で首位、米国籍(198 件)、中国籍(191 件)、欧州籍(183 件)で続いている。製造分野では中国籍の 267 件が最も多く、次いで米国籍(162 件)、日本国籍(153 件)、欧州籍(135 件)となっている(図 4-2-5)。なお、車両分野及び製造分野における日本の技術力マップの拡大係数(成長度を示す指標)は調査国平均を下回っており、この傾向が続けば拡大係数の高い中国、韓国、インド等に追い抜かれる可能性がある(図 4-2-6～図 4-2-13)。

パテントファミリー件数の上位 10 者はすべて米国企業及び中国企業であり、20 位以内に入る日本企業は日本電気と NTT の 2 社のみである(表 4-3-1)。一方、国際パテントファミリー件数で見ると、日本電気と NTT がそれぞれ 4 位、5 位に入り、上位 10 者のうち中国企業は 2 位の華為技術のみとなる。これは中国企業が自国内での出願に重点を置く傾向が強いためと考えられる(表 4-3-2)。

以上のことから、2017 年から 2023 年にかけてサイバー攻撃検知技術の特許出願規模は拡大し、技術開発活動が活発化していることが確認できる。また、米国籍の出願人による出願数が減少する一方で中国籍やインド国籍による出願数が大幅に増加しており、欧州籍、韓国籍及び日本国籍については出願数に大きな変動が見られない。この期間に中国とインドの技術開発活動が著しく活発化したと考えられる。

なお、日本国籍の出願人による出願については、データ収集や脅威情報の分析等の脅威インテリジェンスに関する出願件数や、サイバー攻撃検知技術全般での AI 利用に関する出願件数は、調査国中で下位に位置することが分かった(図 4-4-1、図 4-4-2)。他方、車両分野、製造装置分野に特化したサイバー攻撃検知技術の出願数は調査国中で上位に位置することが確認されたものの、中国やインドの車両分野、製造装置分野の出願件数の伸びは日本より高いため、この傾向が続くようであれば近いうちに車両分野、製造装置分野の出願件数もこれらの国に追い抜かれる可能性があることが分かった。

4. 研究開発動向調査(第５章)の総括

ここでは第５章に掲載した図表を参照して総括を行う。

本調査の調査対象技術である、サイバー攻撃検知技術に関する論文発表件数は、調査期間の 2017 年から 2024 年の間、全体としては増加傾向が認められた(図 5-1-1)。2024 年には 2017 年の 3 倍近い 3,282 件に増加している(図 5-1-1)。

研究者所属機関の国籍・地域別の論文発表件数は、中国籍(世界シェア 24.8%)が最も多く、次いで欧州籍(16.0%)、米国籍(13.7%)、インド国籍(13.5%)、韓国籍(3.1%)、日本国籍(1.3%)の順となっている。特許出願のパテントファミリー件数では、中国籍や米国籍の出願人が目立つが、論文発表件数では、欧州籍が中国籍に次いで 2 位であり、3 位の米国籍よりも存在感を示している。件数の推移に着目すると、中国籍やインド国籍の論文発表件数が大幅に増加している一方、米国籍の論文発表件数は減少傾向である(図 5-1-1)。

技術区分別に注目すると、侵入／異常検知やウイルス／マルウェア検知に AI を利用した検知・判定手法は、全体としては増加傾向が認められた(図 5-2-1)。

研究者所属機関の国籍・地域別の侵入／異常検知やウイルス／マルウェア検知に AI を利用した検知・判定手法の論文発表件数比率は、中国籍が最も高く、次いでインド国籍、欧州籍、米国籍、韓国籍、日本国籍の順となっている。論文全体と比べるとインド国籍の割合が大きいのが特徴である(図 5-4-1)。また、サイバー攻撃検知技術の全論文に対する AI を利用した検知手法の論文の比率は、どの国籍・地域も 50%を超えており、AI を利用した検知が一般的になってきたといえる(表 5-4-1)。

サイバー攻撃検知技術のための脅威情報の収集等、脅威インテリジェンスに関連する(小区分：脅威情報・脆弱性情報、又は中区分：脅威インテリジェンス)論文発表件数は、全体としては増加傾向が認められた(図 5-4-2)。研究者所属機関の国籍・地域別の脅威イ

ンテリジェンスに関連する論文発表件数比率は、中国籍が最も多く、次いで欧州籍、インド国籍、米国籍、韓国籍、日本国籍の順となっている(図 5-4-2)。

研究者所属機関の国籍・地域別の車両分野向けサイバー攻撃検知技術の論文発表件数比率は、中国籍が最も多く、次いで欧州籍、米国籍、韓国籍、インド国籍、日本国籍の順となっている(図 5-4-3)。製造装置分野向けサイバー攻撃検知技術の論文発表件数比率は、車両向けと同じく中国籍が最も多く、次いで欧州籍、米国籍、インド国籍、韓国籍、日本国籍の順となっている(図 5-4-4)。日本国籍は、特許出願のパテントファミリー件数では、車両分野向けのサイバー攻撃検知技術で首位、製造装置向けのサイバー攻撃検知技術で 3 位であったが、論文発表件数では、どちらもインド国籍、韓国籍より低く 6 位である(図 5-4-3、図 5-4-4)。

論文発表件数上位 20 者の所属機関国籍は、中国籍(11 者)とインド国籍(4 者)で 3/4 を占めている(表 5-3-1)。インド国籍の機関は調査期間の前半(2017 年から 2020 年)では 10 位以内に 1 者しか入っていないが、後半(2021 年から 2024 年)では 10 位以内に 4 者が入っている(表 5-3-2)。

以上のことから、2017 年から 2024 年を通じてサイバー攻撃検知技術の論文発表件数の規模は拡大し研究開発活動が活発化していること、米国の論文発表件数が減少し中国やインド、その他の国の論文発表件数が大幅に増加していることが分かった。

なお、日本国籍の論文発表については、サイバー攻撃検知技術の論文発表件数が全体的に少ないことが分かった。脅威インテリジェンスに関する論文発表件数、サイバー攻撃検知技術全般での AI 利用に関する論文発表件数、車両や製造装置分野を含む産業用途のサイバー攻撃検知技術の論文発表件数は、どれも調査国中 6 位で下位に位置している(図 5-4-1～図 5-4-4)。

第２節　示唆

第 1 節で示した調査内容の総括を前提として、日本が今後留意する必要がある方向性を示唆としてまとめた[105]。

我が国のセキュリティ政策については、2014 年 11 月にサイバーセキュリティ基本法が制定され、同法によって、セキュリティ政策に係る政府の司令塔として、サイバーセキュリティ戦略本部が位置付けられた。さらにサイバーセキュリティ対策の強化のため 2025 年 7 月に内閣官房情報セキュリティセンター(NISC)が内閣総理大臣を本部長とする国家サイバー統括室(NCO)に改組され、この新たな体制の下、我が国のサイバーセキュリティ確保に向けた対応も新たなフェーズに入ることとなった。同年 12 月には、諸施策の目標や実施方針を取りまとめたサイバーセキュリティ戦略(2025 年 12 月 23 日閣議決定)が策定され、関係者の共通の理解と行動の基礎が示されている。

また、セキュリティ技術分野の研究開発、技術開発については、経済安全保障の確保・強化の観点から、我が国が支援対象とすべき重要技術の研究開発を進めることとしている「経済安全保障重要技術育成プログラム」の一環として、国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)が実施する「先進的サイバー防御機能・分析能力強化」等において、サイバー空間の情報を収集・調査する状況把握力の向上やサイバー攻撃から機器やシステムを守る防御力の向上に向けた研究開発が取り上げられている。

本調査が取りまとめる「示唆」は、特許出願動向や研究開発動向からみた、我が国が推進するセキュリティ政策やセキュリティ技術分野の研究開発、技術開発に対する助言的な情報提供である。

示唆 1：
日本の脅威インテリジェンス分野では、国外依存と研究開発停滞が同時に続いていることから、日本国内に脅威インテリジェンスを蓄積する仕組みを整備し、国産技術・サービスを核とした、技術、人材を育成する好循環のエコシステムの形成を進めてはいかがか。

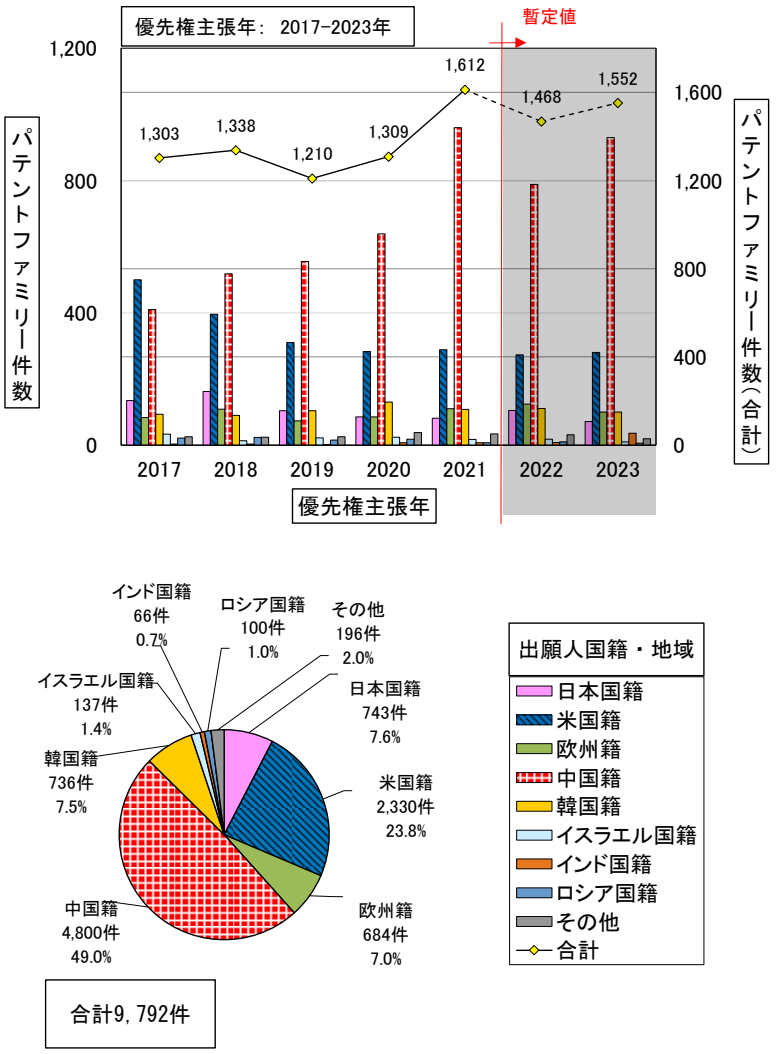
本調査の結果から、脅威インテリジェンスに関する区分が付与された日本国籍の出願人のパテントファミリーで優先権主張年が 2017 年～2023 年であるものの件数は 743 件でシェア 7.6%(調査国中 3 位)であることが分かった。また、パテントファミリー件数の年次推移によると日本国籍の出願人の件数は 2017 年の 135 件から 2021 年の 81 件へと大きく減少している。一方、中国籍の出願人の件数は同じ期間に 410 件(2017 年)から 960 件(2021 年)と 2 倍以上に増加している。また、欧州籍の出願人の件数は 83 件(2017 年)から 110 件(2021 年)、韓国籍の出願人の件数は 93 件(2017 年)から 108 件(2021 年)へと増加している。その結果、2017 年から 2021 年の間に日本国籍の出願人のパテントファミリー件数のシェアは 10.4%から 5.0%に半減し、調査国全体の中での日本の順位が低下している(表 6-2-1、図 6-2-1)。

[105] 本節において参照する図表はすべて初出が本節より前のものであるが、理解のしやすさを考慮し、一部分は本節が含まれる第 6 章の番号を付して明示している。

表 6-2-1　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率(脅威インテリジェンス)(表 4-4-2 再掲)

パテントファミリー件数	優先権主張年							合計	比率
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023		
合計	1,303	1,338	1,210	1,309	1,612	1,468	1,552	9,792	100.0%
日本国籍	135	162	104	85	81	105	71	743	7.6%
米国籍	500	396	310	283	288	273	280	2,330	23.8%
欧州籍	83	109	73	85	110	124	100	684	7.0%
中国籍	410	518	555	639	960	788	930	4,800	49.0%
韓国籍	93	90	104	130	108	111	100	736	7.5%
イスラエル国籍	33	13	22	24	17	18	10	137	1.4%
インド国籍	3	3	2	7	7	8	36	66	0.7%
ロシア国籍	21	23	15	18	7	10	6	100	1.0%
その他	25	24	25	38	34	31	19	196	2.0%
日本国籍の全件数に対する比率	10.4%	12.1%	8.6%	6.5%	5.0%	7.2%	4.6%	7.6%	

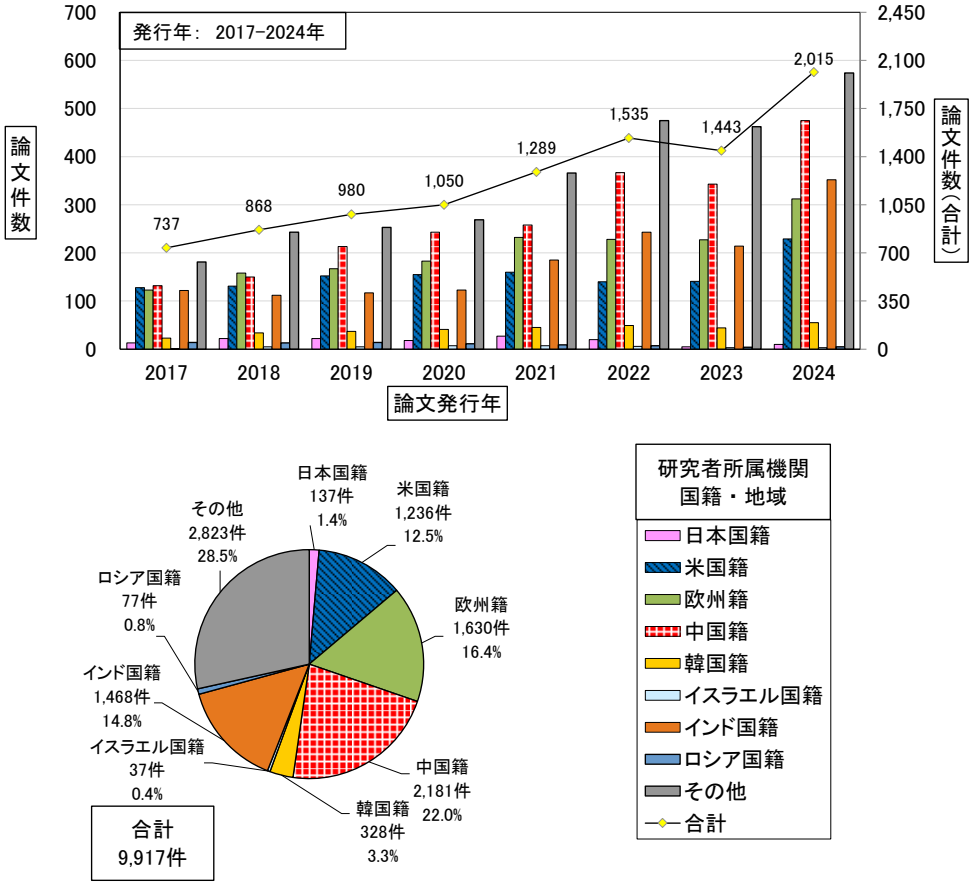
図 6-2-1　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率(脅威インテリジェンス)(図 4-4-1 再掲)



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

また、脅威インテリジェンスに関する区分が付与された日本国籍の研究者所属機関の論文で論文発行年が 2017 年～2024 年であるものの発表件数は 137 件でシェア 1.4%(調査国中 6 位)であり、特許と比べてもシェアは低い状況である(図 6-2-2)。

図 6-2-2 ［研究者所属機関国籍・地域別］論文発表件数年次推移及び論文発表件数比率(脅威インテリジェンス(小区分：脅威情報・脆弱性情報、中区分：脅威インテリジェンス))(図 5-4-2 再掲)



なお、有識者からは、日本向け攻撃キャンペーンや日本のビジネス環境特有のニーズが存在することから、海外の脅威インテリジェンスを日本にそのまま適用できるものではない、日本企業の脅威インテリジェンスの分析能力は他国に比べて必ずしも低くない、といった意見が表明された。さらに、市場動向調査により、日本のサイバーセキュリティ市場では、製品・サービスともに国外ベンダの製品の寡占が進んでおり、例えば SIEM のシェアは 85%以上が国外ベンダに占められていることが判明した。これを背景に、日本国内においては海外ベンダの製品を利用せざるを得ない状況であることが複数の有識者により指摘された。

これらを踏まえ、安全保障の観点から、サイバーセキュリティ戦略において示されているように、海外の技術やサービスに過度に依存しないことを目指すのであるとすれば、国産技術・サービスを核とした、技術、人材を育成する好循環のエコシステムの基礎となる脅威インテリジェンスを日本にも蓄積することが必要となると考えられる。

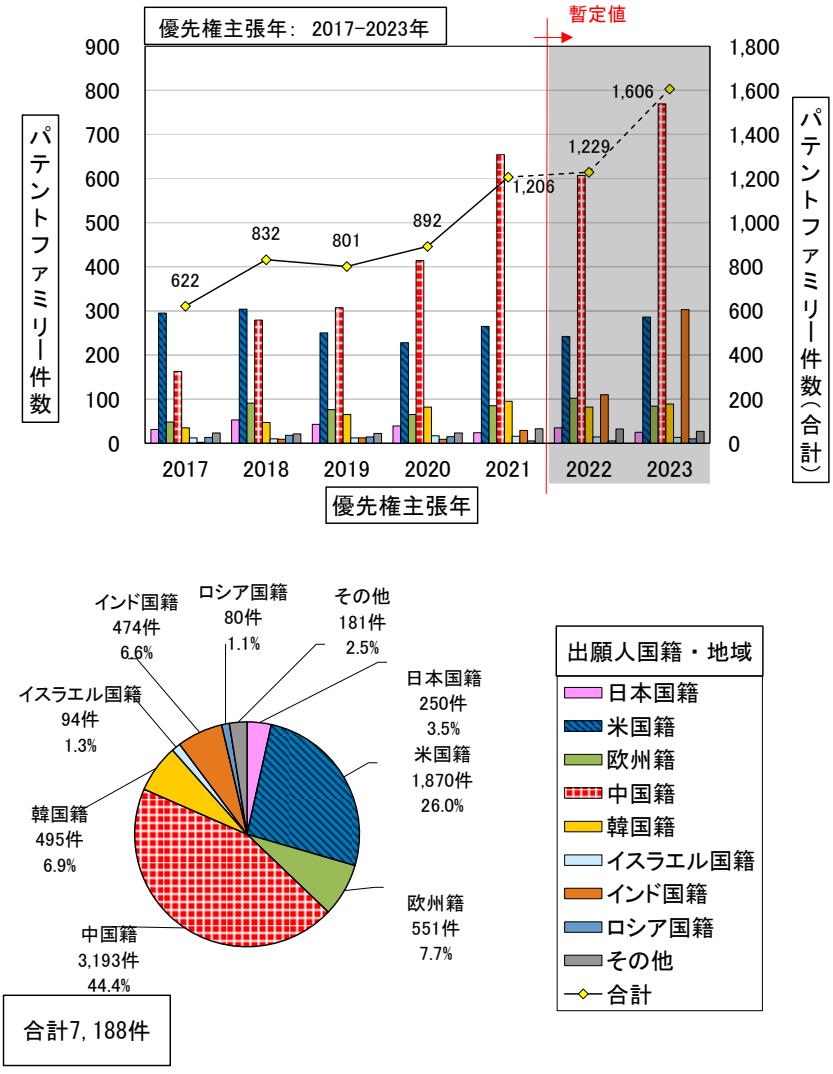
以上のことから、日本国内に脅威インテリジェンスを収集・分析する仕組みを整備すること、および、収集した脅威インテリジェンスに対して日本企業の分析能力を発揮することにより、日本市場に適応した製品を開発していくことが重要であると考えられる。

そして、脅威インテリジェンスに関する区分が付与されたパテントファミリー件数の日本のシェア 7.6%は、世界シェアとしては高くないものの(表 6-2-1)、全出願に対するパテントファミリー件数の日本のシェア 6.4%よりは高く(図 4-1-1)、既に日本としてもこの分野に力を入れ始めているように見受けられる。また、一般的に先行して研究開発を行うことにより将来利益を得る可能性が高まると期待できることから、この技術分野を中心としたエコシステムが構築され、日本市場に適応した製品の開発へとつながるよう、特許出願や論文発表がより活発に行われることが推奨される。

なお、アドバイザリーボードの委員からは、日本国内に脅威インテリジェンスを蓄積することも重要であるが、製品開発はグローバルで通用する技術を実現するための一部の要素に過ぎず、むしろ普及施策が非常に重要であるとの意見があった。また、ユーザ企業は機能や技術面よりも、これまでの利用実績を重視する傾向にあるため、商流の中心であるシステムインテグレーター(以下、SI 事業者)が国内製品・サービスをより積極的に取り上げていくべきであるとの意見もあった。そのためには、政府機関による調達を通じた実績作りや SI 事業者とベンダのマッチングによる国産製品の認知・活用の機会の促進等、商流の中心である SI 事業者が国産製品を採用する土壌づくりを進めることが効果的ではないか。

また、有識者ヒアリングからは、脅威インテリジェンスに限るものではないが、現状は人手により行われている SOC(Security Operation Center)業務、インシデント対応、脅威分析等では、今後、大幅な人手不足が見込まれているところ、こうした人手不足を解消して、分析すべきデータの増加に対処するためにも、AI の利用の促進が求められるという意見が得られている。AI を利用した検知判定手法の世界全体のパテントファミリー件数は 2017 年の 622 件から 2023 年には 1,606 件とおよそ 2.5 倍(図 6-2-3)、AI を利用した検知判定手法の世界全体の論文発表件数は 2017 年の 434 件から 2024 年には 2,410 件とおよそ 5.5 倍に増えている(図 5-4-1)。一方で、AI を利用した検知判定手法に区分が付与された日本国籍の出願人のパテントファミリー件数は 250 件でシェア 3.5%(調査国中 6 位)であり(図 6-2-3)、AI を利用した検知判定手法に区分が付与された日本国籍の研究者所属機関の論文発表件数は 117 件でシェア 1.2%(調査国中 6 位)(図 5-4-1)であり、どちらも調査国中下位であった。なお、サイバーセキュリティ戦略においても、AI を活用したサイバー攻撃インフラの検知や関連情報の分析の精緻化・迅速化等を推進すると記載されている。また、脅威分析においては、国内の脅威情報に応じた分析が必要となるため、日本の企業や研究機関による AI 利用技術に関する研究が欠かせないと思われる。

図 6-2-3　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率(AI を利用した検知判定手法)(図 4-4-2 再掲)



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

示唆 2：

重要インフラ分野[106]、基幹インフラ分野[107]又は国際競争力を有する産業[108]向けのサイバー攻撃検知技術において、日本が占めるシェア、国際比較における日本の注力度や成長度を考慮して、特許出願及び研究開発を進めてはいかがか。

例えば、他国にシェアで追い越される可能性のある技術(車両分野向け、製造装置分野向け)や今後他国にシェアで差を広げられるおそれのある技術(情報通信分野向け、電力分野向け)においては、より積極的な特許出願及び研究開発を行い、また、さらに現状では日本が弱いものの、一定の成長が見られる技術(医療分野向け、金融分野向け)においては、引き続き特許出願及び研究開発を続けることが効果的ではないか。

重要インフラ分野を含む特定産業向けサイバー攻撃検知技術の区分が付与された世界全体のパテントファミリーで優先権主張年が 2017 年～2023 年であるものの件数は、産業分野別に降順で挙げると、情報通信(1,396 件、うち日本国籍シェア 11.0%)、車両(1,010 件、26.8%)、製造装置(805 件、19.0%)、金融(780 件、3.7%)、電力(534 件、7.3%)、医療(269 件、4.8%)、交通システム(227 件、15.4%)、クレジット(126 件、7.1%)、政府・行政サービス(117 件、6.8%)、航空(112 件、3.6%)、水道(85 件、17.6%)、教育(78 件、2.6%)、物流(74 件、9.5%)、化学(71 件、11.3%)、ガス(61 件、16.4%)、鉄道(54 件、18.5%)、石油(53 件、5.7%)、学術研究(40 件、5.0%)、空港(18 件、5.6%)、港湾(9 件、0.0%)である(図 6-2-4、表 6-2-2)。

これらの件数を降順で累積していくと、全分野の件数の合計(5,919 件)の 80%以上となる最小個数の分野の集合は、情報通信、車両、製造装置、金融、電力及び医療の 6 分野である。以下、この 6 分野に絞って、日本国籍出願人のパテントファミリー件数のシェアが高い順に検討する。

表 6-2-2 ［出願先：日米欧中韓以印露 WO］特定産業向けサイバー攻撃検知技術のパテントファミリー件数(日本国籍の順位・出願比率)(表 4-4-4 再掲)

産業分野	物流	電力	鉄道	石油	政府・行政サービス	水道	情報通信	航空	港湾	空港
順位(日本国籍)	3	3	3	5	4	3	3	5	6	4
出願比率(日本国籍)	9.5%	7.3%	18.5%	5.7%	6.8%	17.6%	11.0%	3.6%	0.0%	5.6%

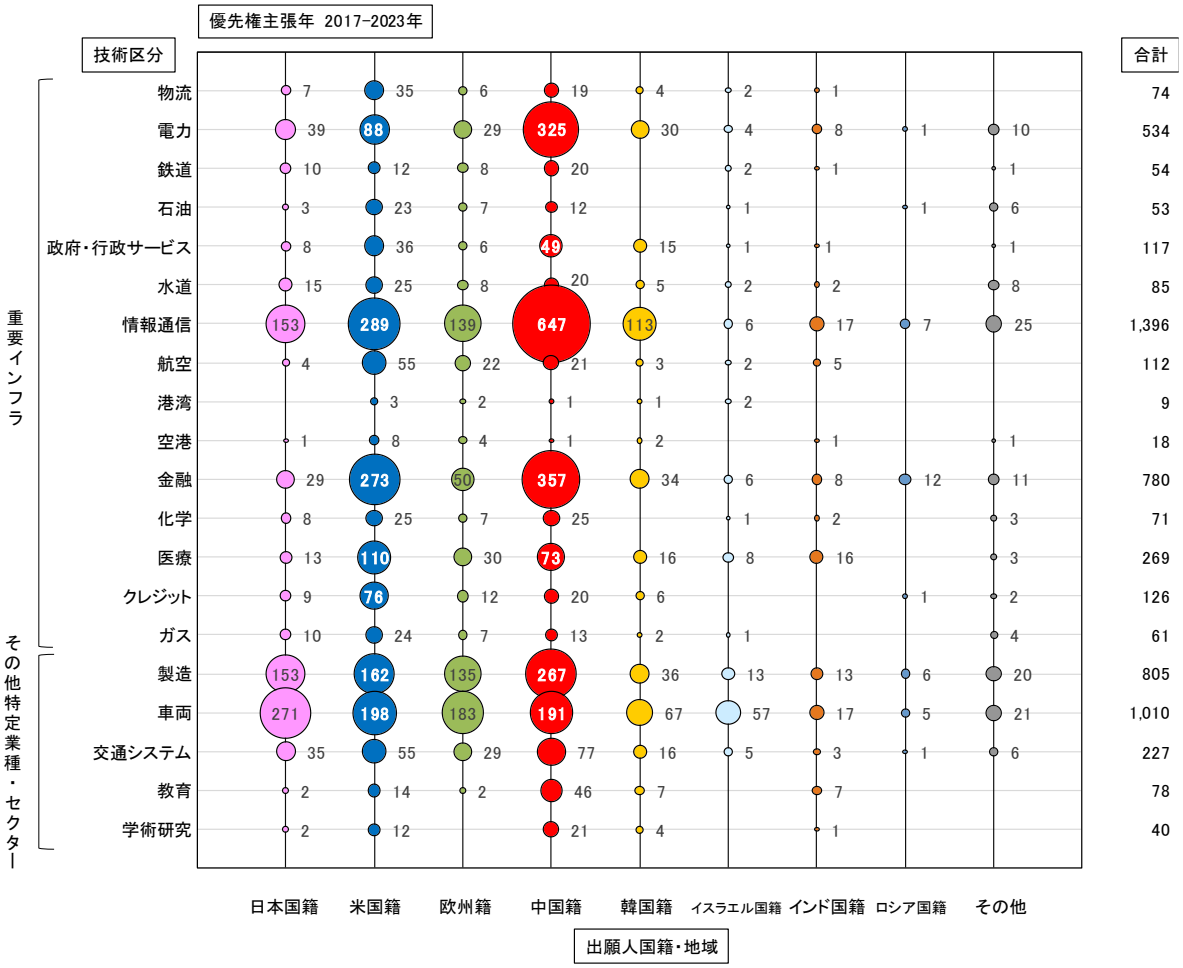
産業分野	金融	化学	医療	クレジット	ガス	製造	車両	交通システム	教育	学術研究
順位(日本国籍)	5	3	6	4	3	3	1	3	5	4
出願比率(日本国籍)	3.7%	11.3%	4.8%	7.1%	16.4%	19.0%	26.8%	15.4%	2.6%	5.0%

[106] 重要インフラのサイバーセキュリティに係る行動計画(2025 年改定)の別紙 1 に示されている、「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス」「医療」「水道」「物流」「化学」「クレジット」「石油」及び「港湾」の 15 分野。

[107] 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(経済安全保障推進法)において特定社会基盤事業として指定されている、「電気」「ガス」「石油」「水道」「鉄道」「貨物自動車運送」「外航海運」「港湾」「航空」「空港」「電気通信」「放送」「郵便」「金融」及び「クレジットカード」の 15 分野。

[108] 例えば「自動車」「半導体等電子部品」「鉄鋼」「自動車の部分品」及び「半導体等製造装置」(対世界主要輸出品(2023 年、財務省貿易統計)の上位 5 品目)の産業。

図 6-2-4 ［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］パテントファミリー件数（重要インフラ、その他特定業種・セクター、優先権主張年：2017-2023年）（図 4-2-5 再掲）



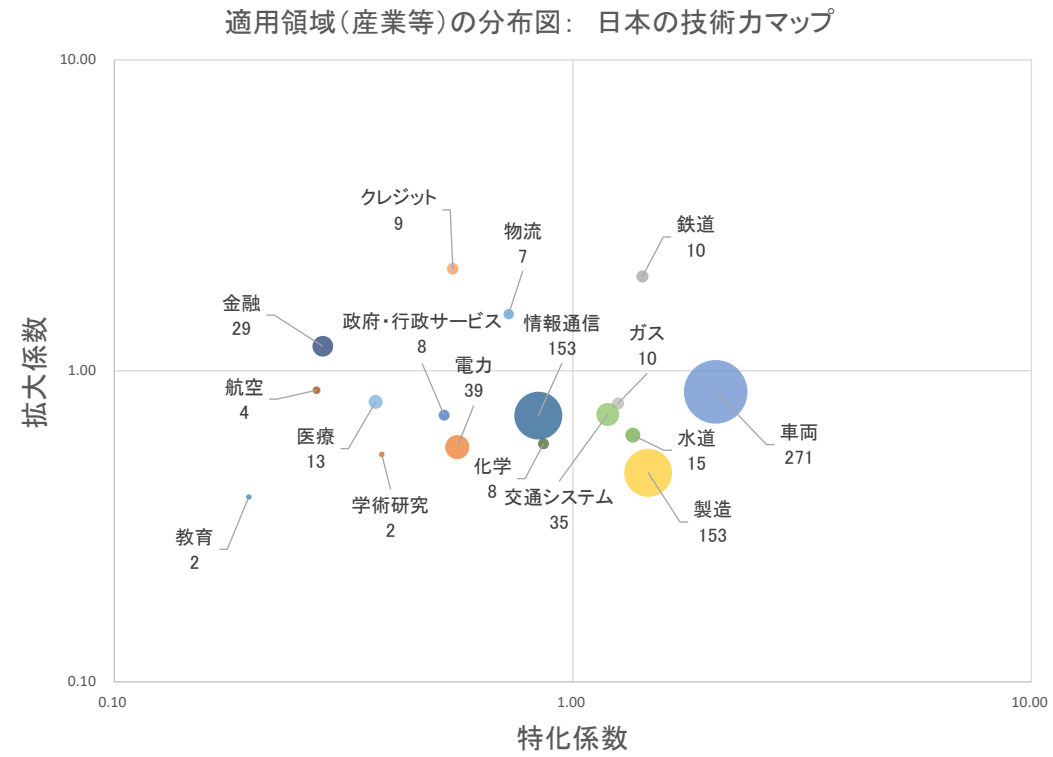
車両分野向け及び製造装置分野向けのサイバー攻撃検知技術において、日本国籍出願人のパテントファミリー件数のシェアは、それぞれ 26.8%及び 19.0%であり、いずれも高いシェアを示している。全出願に対する日本国籍出願人のシェアである 6.4%を大きく上回っているため、日本はこれらの分野に非常に注力しており、現状は日本の強みがある分野である（表 6-2-2、図 4-1-1）。車両分野向けサイバー攻撃検知技術の特許出願数上位 20 者中、8 者が日本国籍であり、上位にはパナソニック（1 位）、デンソー（3 位）等が入っている（表 4-4-5）。製造装置分野向けサイバー攻撃検知技術の特許出願数上位 20 者中、8 者が日本国籍であり、上位には日立製作所（2 位）、三菱電機（2 位）等が入っている（表 4-4-6）。

一方、日本国籍出願人のパテントファミリー件数の増減に着目すると、成長度を示す指標である拡大係数が 1 未満であり、増加率は他国を下回っている（日本の技術力マップ（図 6-2-5）の拡大係数）。日本国籍出願人のパテントファミリー件数比率の推移を見ると、車両分野向けでは、2017 年（26.7%）から 2018 年（35.1%）まで上がった後に 2021 年（23.1%）まで減少しており、製造装置分野向けでは、2017 年（31.4%）をピークに 2021 年（15.8%）まで減少している。中国籍出願人のパテントファミリー件数比率は、車両分野向け及び製

造装置分野向けのいずれにおいても、2017 年から 2021 年にかけて大きく増加している(表 6-2-3、表 6-2-4)。このため、この傾向が続けば、日本は中国にパテントファミリー件数のシェアにおいて逆転されるおそれがある。

なお、車両分野向けのサイバー攻撃検知技術に関して、車両についてインターネットを介した大規模なサイバー攻撃は現時点で限定的だが、車両に対する深刻なサイバー攻撃(車載システムへのハッキング等)は、今後のコネクテッドカー普及や自動運転車両の普及に伴って拡大する見込みであり、それに先駆けた対策が必要であるという意見が複数の有識者から得られた。また、一部の有識者から、サイバー攻撃の研究開発においては実データの収集が重要であるところ、世界的にシェアが高い日本メーカーの車両をプローブとして情報収集することにより、日本の優位性を生かせる可能性があるとの意見も得られた。

図 6-2-5　[出願先：日米欧中韓以印露 WO][技術区分別]縦軸を拡大係数、横軸を特化係数とした、各技術区分の分布図(技術区分＝適用領域(産業等)、出願人国籍・地域＝日本)(図 4-2-6 再掲)



※拡大係数及び特化係数の定義については、第１章第４節３．を参照されたい。

表 6-2-3 ［出願先：日米欧中韓以印露 WO］[出願人国籍・地域別］パテントファミリー件数比率の年次推移(車両)(表 4-4-7 再掲)

件数比率	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	26.7%	35.1%	25.2%	26.1%	23.1%	30.5%	21.1%	26.8%
米国籍	25.7%	27.2%	25.2%	23.5%	17.7%	10.8%	11.6%	19.6%
欧州籍	19.8%	15.9%	14.4%	19.3%	22.6%	15.0%	19.7%	18.1%
中国籍	3.0%	7.3%	10.1%	16.8%	24.7%	30.5%	31.3%	18.9%
韓国籍	3.0%	2.6%	4.3%	11.8%	8.6%	7.8%	7.5%	6.6%
イスラエル国籍	18.8%	5.3%	15.1%	1.7%	1.1%	0.6%	2.7%	5.6%
インド国籍	1.0%	0.7%	0.7%	0.0%	0.5%	3.6%	4.8%	1.7%
ロシア国籍	0.0%	2.0%	1.4%	0.0%	0.0%	0.0%	0.0%	0.5%
その他	2.0%	4.0%	3.6%	0.8%	1.6%	1.2%	1.4%	2.1%

表 6-2-4 ［出願先：日米欧中韓以印露 WO］[出願人国籍・地域別］パテントファミリー件数比率の年次推移(製造装置)(表 4-4-8 再掲)

出願件数	優先権主張年							合計
出願人国籍・地域	2017	2018	2019	2020	2021	2022	2023	
日本国籍	31.4%	27.6%	26.5%	13.6%	15.8%	13.3%	9.1%	18.9%
米国籍	20.9%	32.4%	18.8%	28.2%	15.8%	14.2%	15.7%	20.4%
欧州籍	25.6%	13.3%	18.8%	9.1%	15.8%	20.0%	14.0%	16.4%
中国籍	15.1%	15.2%	18.8%	30.9%	43.8%	46.7%	53.7%	33.5%
韓国籍	2.3%	4.8%	4.3%	10.9%	4.1%	2.5%	1.7%	4.3%
イスラエル国籍	1.2%	1.9%	5.1%	1.8%	2.7%	0.0%	0.0%	1.9%
インド国籍	0.0%	1.9%	0.0%	0.9%	0.7%	1.7%	4.1%	1.4%
ロシア国籍	0.0%	0.0%	4.3%	0.9%	0.0%	0.0%	0.0%	0.7%
その他	3.5%	2.9%	3.4%	3.6%	1.4%	1.7%	1.7%	2.5%

情報通信分野向け及び電力分野向けのサイバー攻撃検知技術において、日本国籍出願人のパテントファミリー件数のシェアは、それぞれ 11.0%及び 7.3%であり、一定のシェアを有している(表 6-2-2)。いずれの分野も、6.4%(全出願に対する日本国籍出願人のシェア)を上回っているため、日本はこれらの分野に注力しているといえる一方で、注力度を示す指標である特化係数は 1 を下回っているため、各国におけるシェアの平均を下回っており、他国は日本以上に注力しているといえる(図 4-1-1、日本の技術力マップ(図 6-2-5)の特化係数)。

また、日本国籍出願人のパテントファミリー件数の増減に着目すると、拡大係数が 1 を下回っているため、増加率は他国を下回っている(日本の技術力マップ(図 6-2-5)の拡大係数)。日本国籍出願人のパテントファミリー件数比率の推移を見ると、情報通信分野向けでは、2017 年(14.7%)をピークに 2021 年(9.5%)まで減少しており、電力分野向けでは、2017 年(20.0%)をピークに 2021 年(7.8%)まで減少している。中国籍出願人のパテントファミリー件数比率は、情報通信分野向け及び電力分野向けのいずれにおいても、2017 年から 2021 年にかけて大きく増加している(表 4-4-9、表 4-4-10)。

医療分野向け及び金融分野向けのサイバー攻撃検知技術において、日本国籍出願人のパテントファミリー件数のシェアは、それぞれ 4.8%及び 3.7%であり、現状は日本が弱い分野である。いずれの分野も、6.4%(全出願に対する日本国籍出願人のシェア)を下回っており、日本は他分野より注力していない(表 6-2-2、図 4-1-1)。

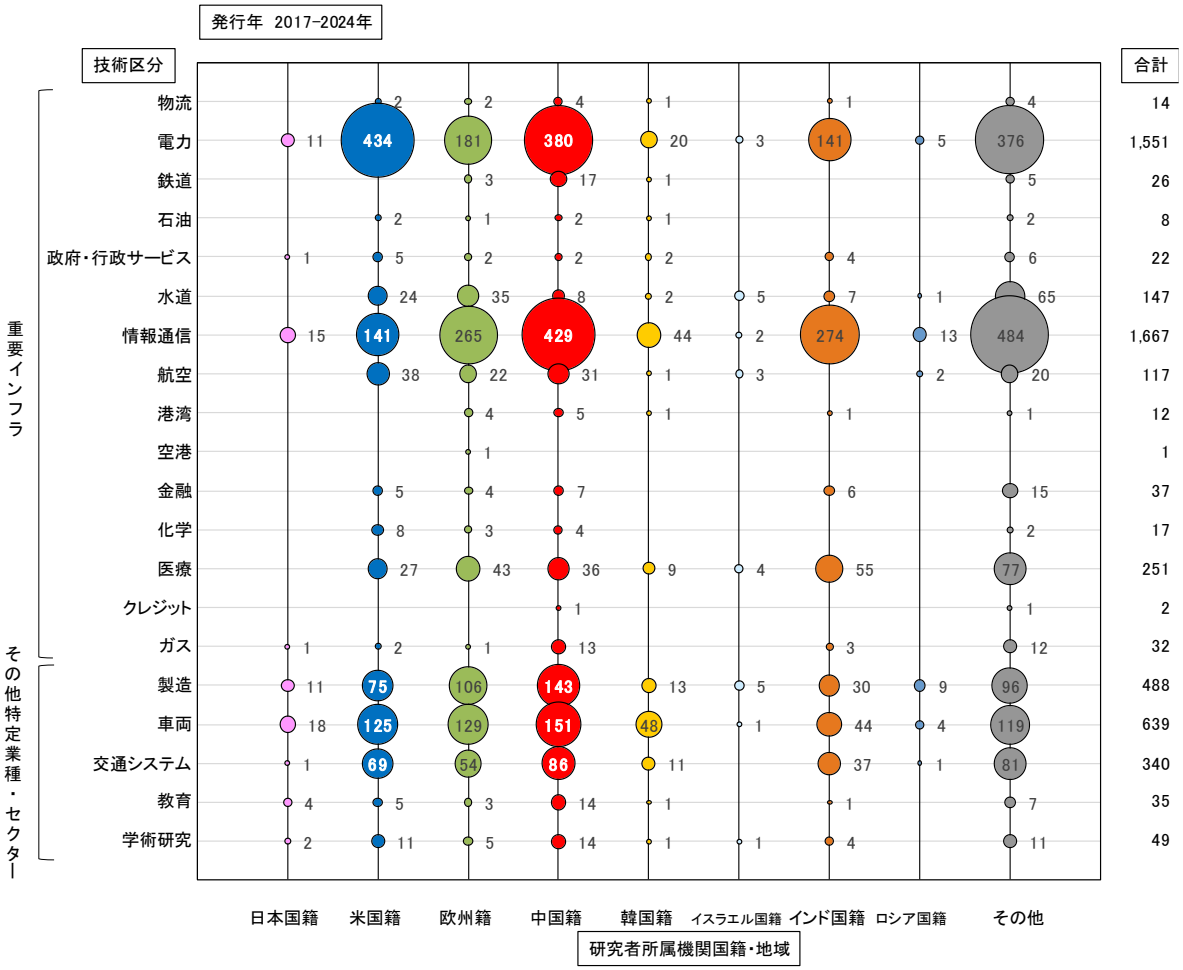
一方、日本国籍出願人のパテントファミリー件数の増減に着目すると、医療は拡大係数が 1 以下、金融は 1 以上であることから、金融については一定の成長が見られる(日本の技術力マップ(図 6-2-5)の拡大係数)。日本国籍出願人のパテントファミリー件数比率の推移を見ると、医療分野向けでは、2017 年(3.8%)、2018 年(8.0%)、2019 年(3.0%)、

2020 年(2.4%)、2021 年(7.0%)と増減を繰り返しており減少傾向は見られない。金融分野向けでは、2017 年(2.1%)から 2021 年(6.3%)までおおむね増加している。中国籍出願人のパテントファミリー件数比率は、医療分野向け及び金融分野向けのいずれにおいても、2017 年から 2021 年にかけて大きく増加している(表 4-4-11、表 4-4-12)。

重要インフラ分野を含む特定産業向けサイバー攻撃検知技術の区分が付与された日本国籍の研究者所属機関の論文で論文発行年が 2017 年～2024 年であるものの発表件数は、いずれの産業分野においても調査対象国の中で順位が低く、おおむね 6 位以下である(図 6-2-6)。

なお、一部の有識者からは、日本のサイバーセキュリティ研究は、研究者数が少なく、産業界とアカデミアの距離が離れていて共同研究等の絶対数が少なく、大学や国研等の機関で実践的な研究を行っている例が少ないのが実情であるとの意見もあった。

図 6-2-6 ［技術区分別－研究者所属機関国籍・地域別］論文発表件数(重要インフラ、その他特定業種・セクター)(図 5-2-6 再掲)



仮に、サイバーセキュリティ戦略(2025 年 12 月 23 日閣議決定)が示すように、重要インフラ・基幹インフラやサプライチェーン全体におけるサイバーセキュリティの向上とサイバーセキュリティ対策技術の海外依存の低減とを目指すのであるとするならば、例

えば重要インフラ分野向けサイバー攻撃検知技術や国際競争力を有する産業向けのサイバー攻撃検知技術が、国内で持続的に開発され、日本の強みとなることが望ましいと言えるであろう。

以上を総合すると、重要インフラ分野、基幹インフラ分野又は国際競争力を有する産業向けのサイバー攻撃検知技術においては、日本が占めるシェア、国際比較での日本の注力度(特化係数)や成長度(拡大係数)に応じて、特許出願及び研究開発を進めることが有用であろう。

とりわけ、現状では日本の強みであるが、他国にシェアで追い越される可能性のある技術(例えば、車両分野向け、製造装置分野向け)については、日本の強さを維持できるように、特許出願及び研究開発の強化を行うことが効果的であろう。また、国際比較では注力度が低く、今後他国にシェアで差を広げられるおそれのある技術(例えば、情報通信分野向け、電力分野向け)については、他国に差を付けられないように、積極的な特許出願及び研究開発を行う必要があると考えられる。さらに、現状では日本が弱いものの、一定の成長が見られる技術(例えば、医療分野向け、金融分野向け)については、引き続き、特許出願及び研究開発を続けることが必要であると考えられる。

なお、アドバイザリーボードの複数の委員からは、研究開発と市場創出の加速に向けて、引き続き日本発技術の普及を後押しする施策の推進を政府に求めたいとの意見があった。また、サイバーセキュリティ分野全体にわたって、産学連携のハードルが高いとの認識が示され、実効的な形で連携が後押しされることに期待が寄せられた。

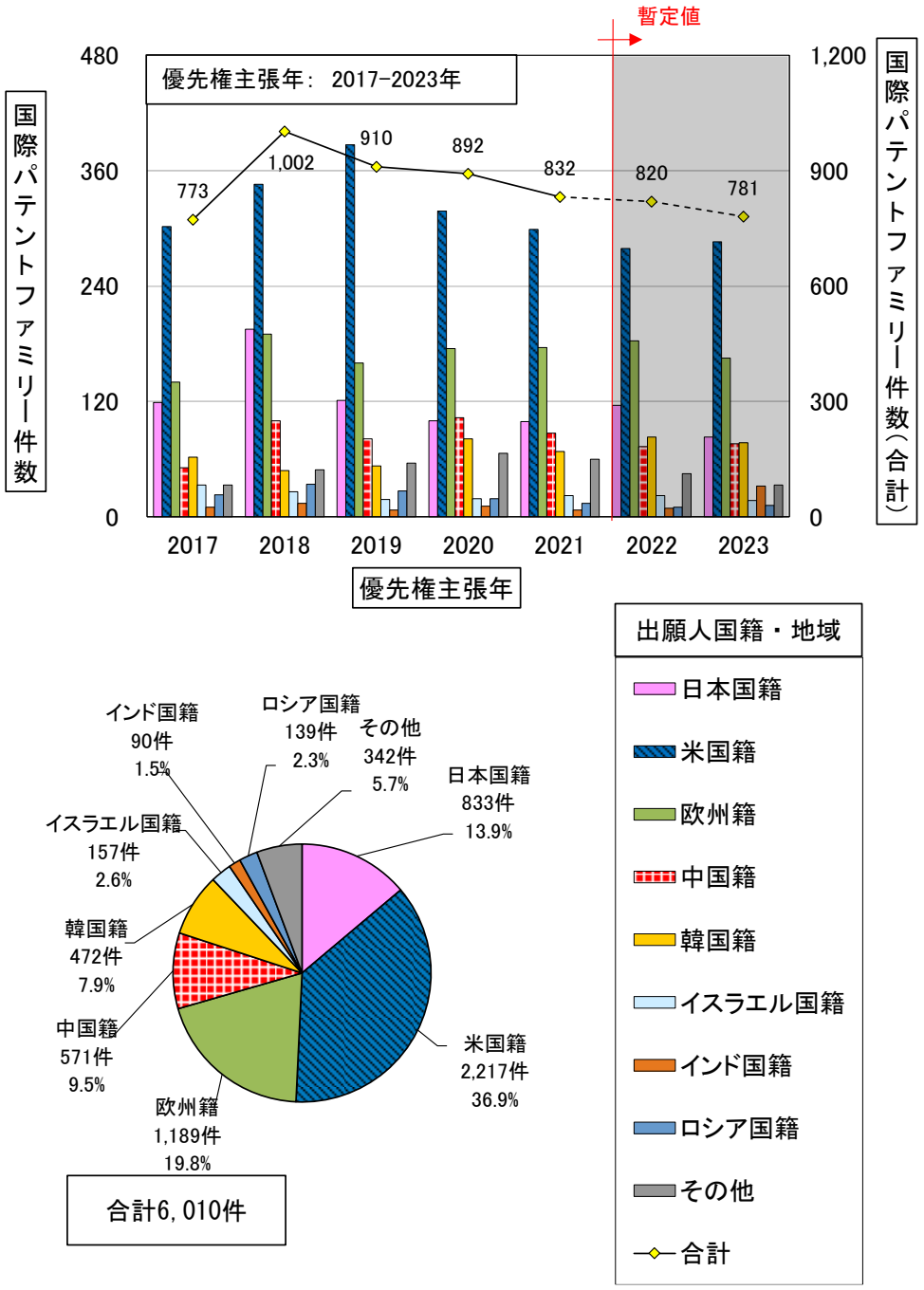
参考図表

１．　特許動向調査に関する参考図表

（１）　国際パテントファミリー件数に関する参考図表

①　［出願人国籍・地域別］国際パテントファミリー件数年次推移および件数比率

図-参考-1　［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］［IPF］国際パテントファミリー件数年次推移および国際パテントファミリー件数比率



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

② ［技術区分別－出願人国籍・地域別］国際パテントファミリー件数

図-参考-2 ［出願先：日米欧中韓以印露 WO］［技術区分別－出願人国籍・地域別］［IPF］国際パテントファミリー件数（大区分：適用領域、解決課題／効果、AI に対する攻撃対策、脅威インテリジェンス、優先権主張年：2017-2023 年）

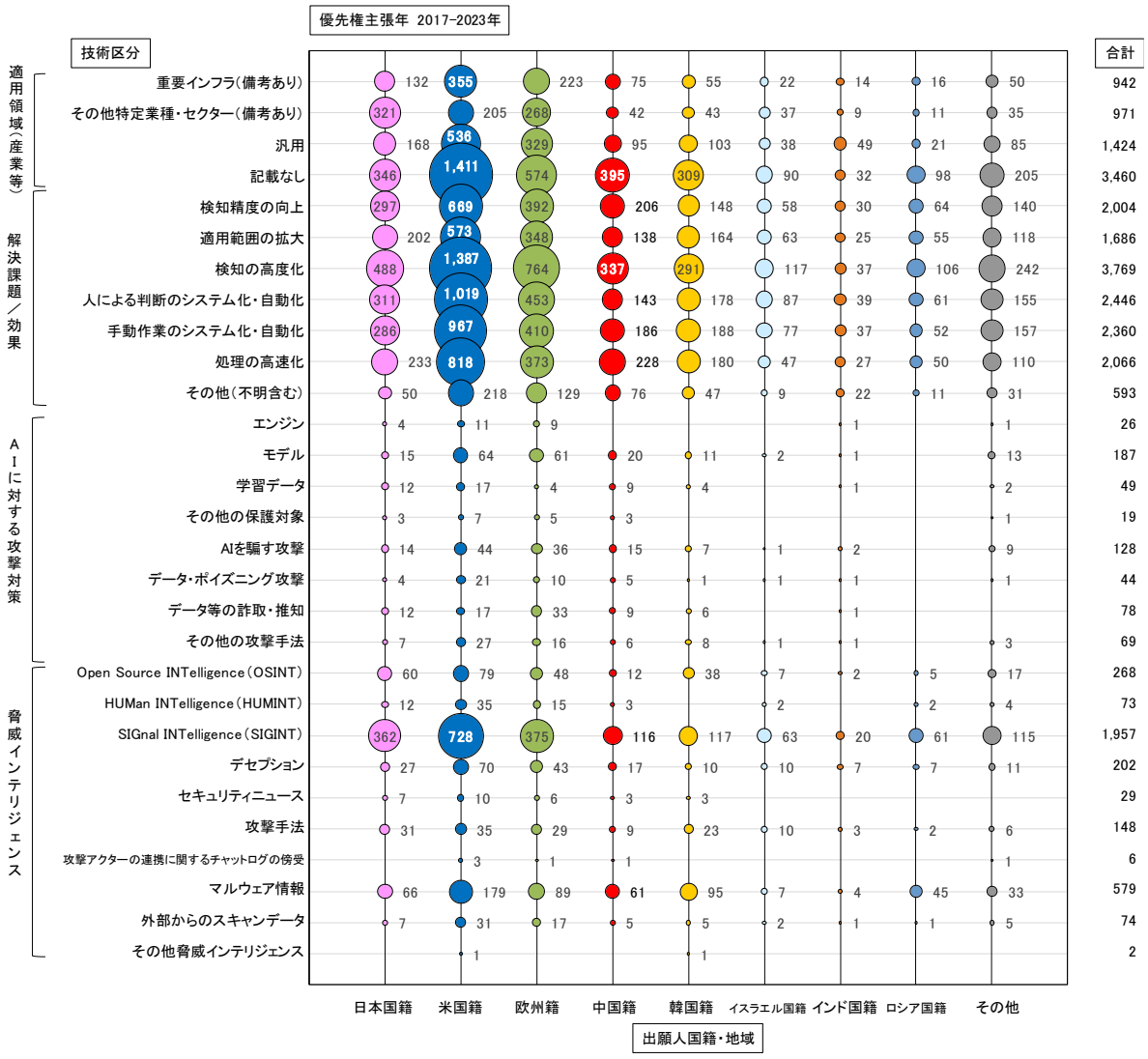
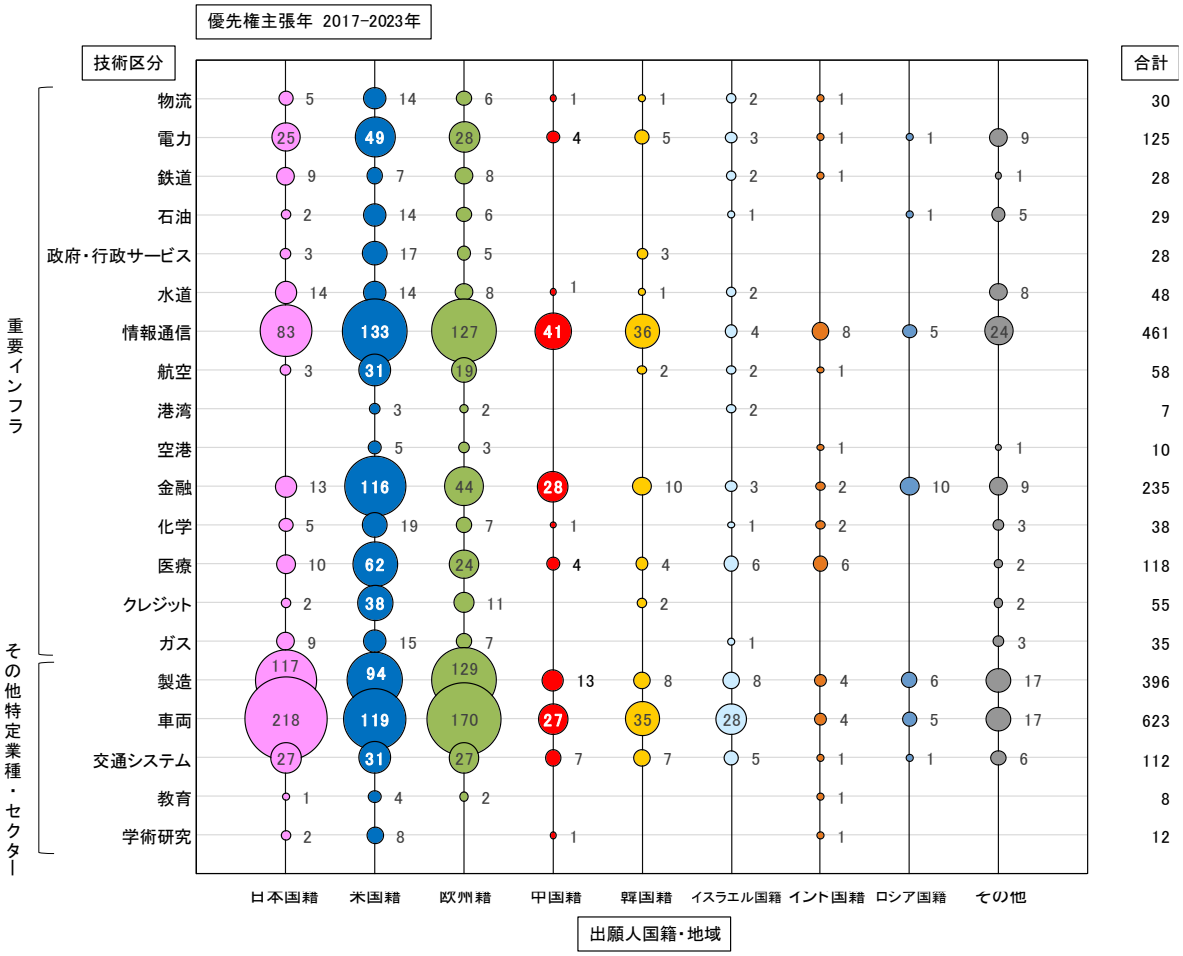


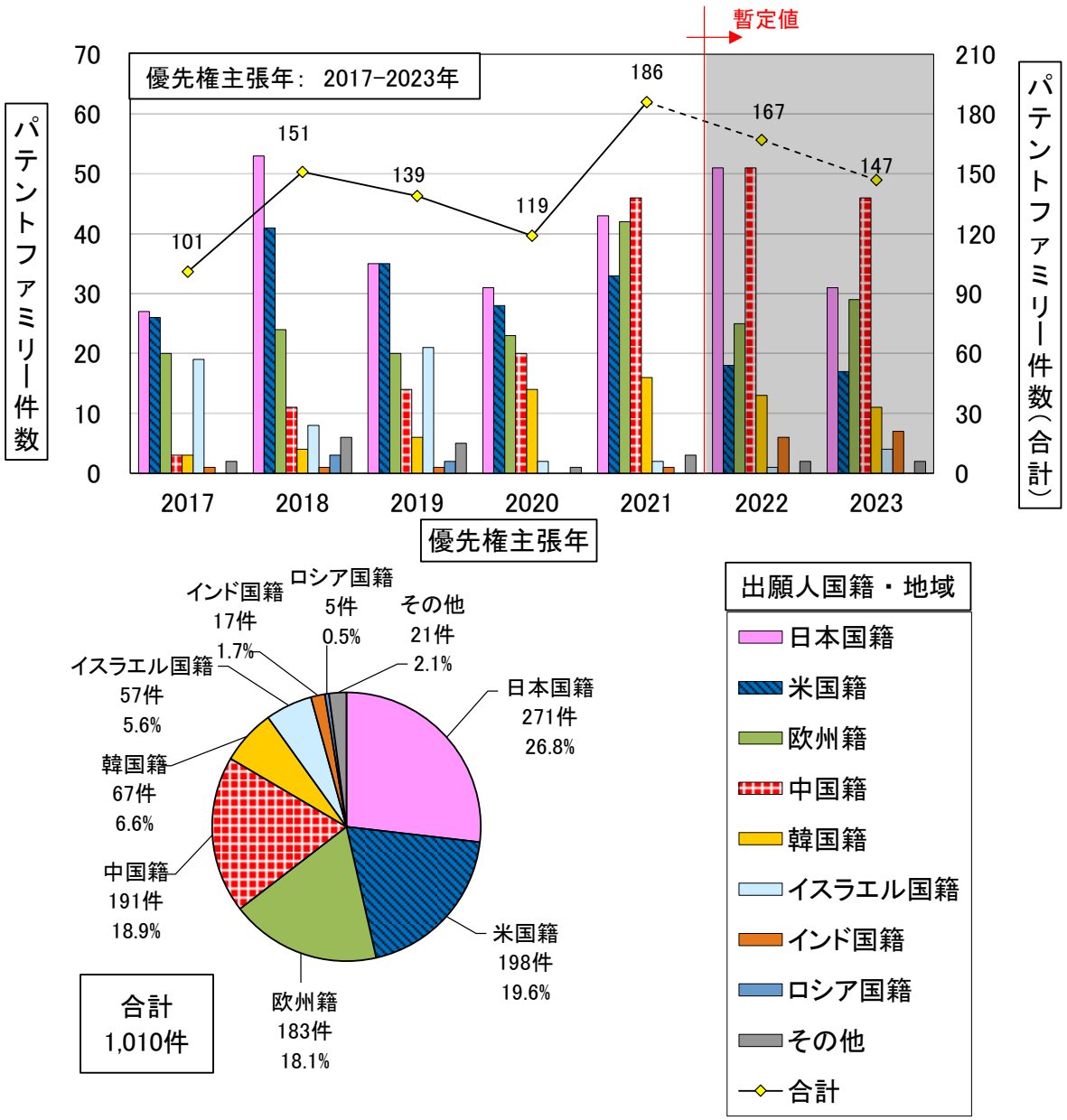
図-参考-3　[出願先：日米欧中韓以印露 WO][技術区分別－出願人国籍・地域別][IPF]国際パテントファミリー件数（重要インフラ～その他特定業種・セクター、優先権主張年：2017-2023 年）



（２）　パテントファミリー件数に関する参考図表

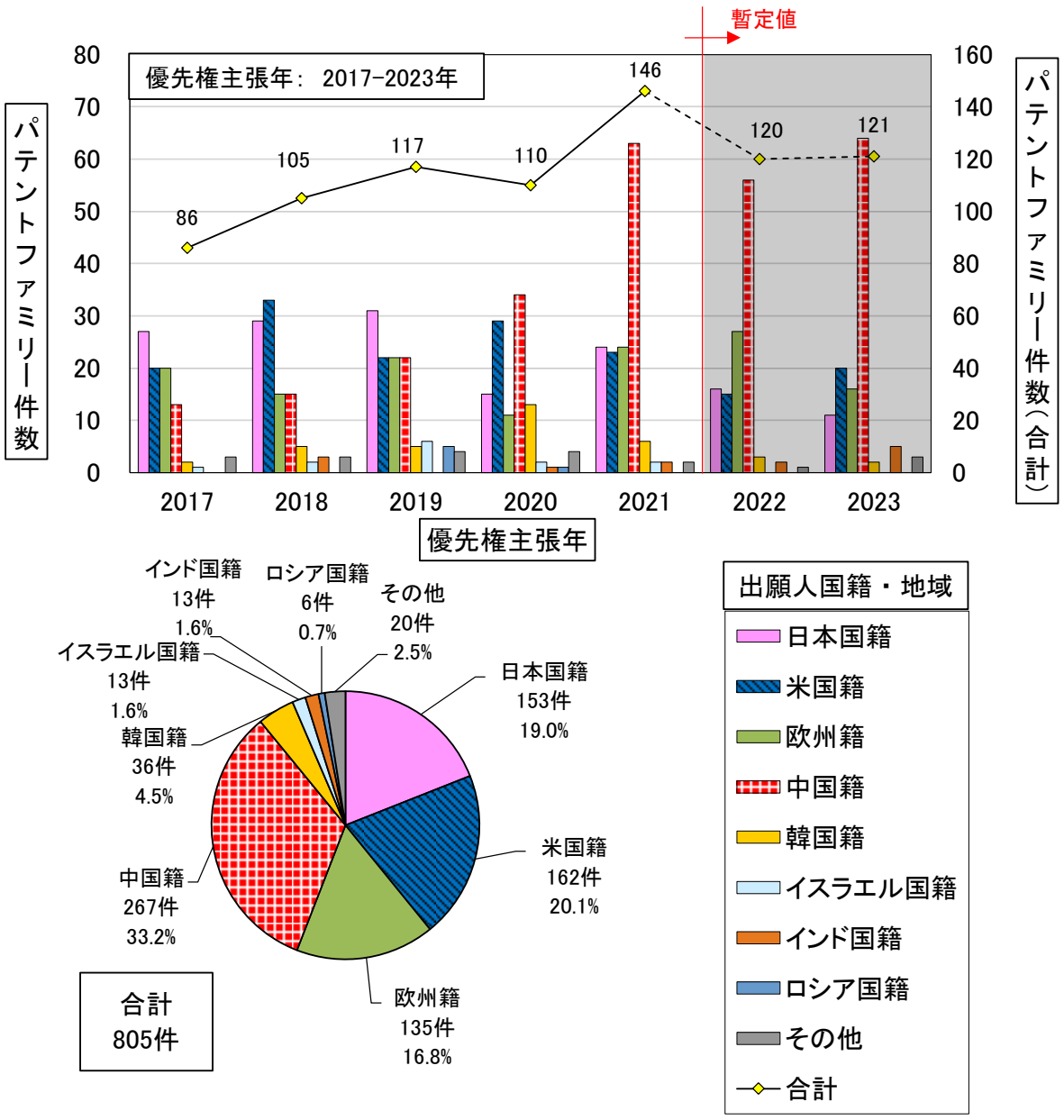
①　［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率

図-参考-4　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝車両）



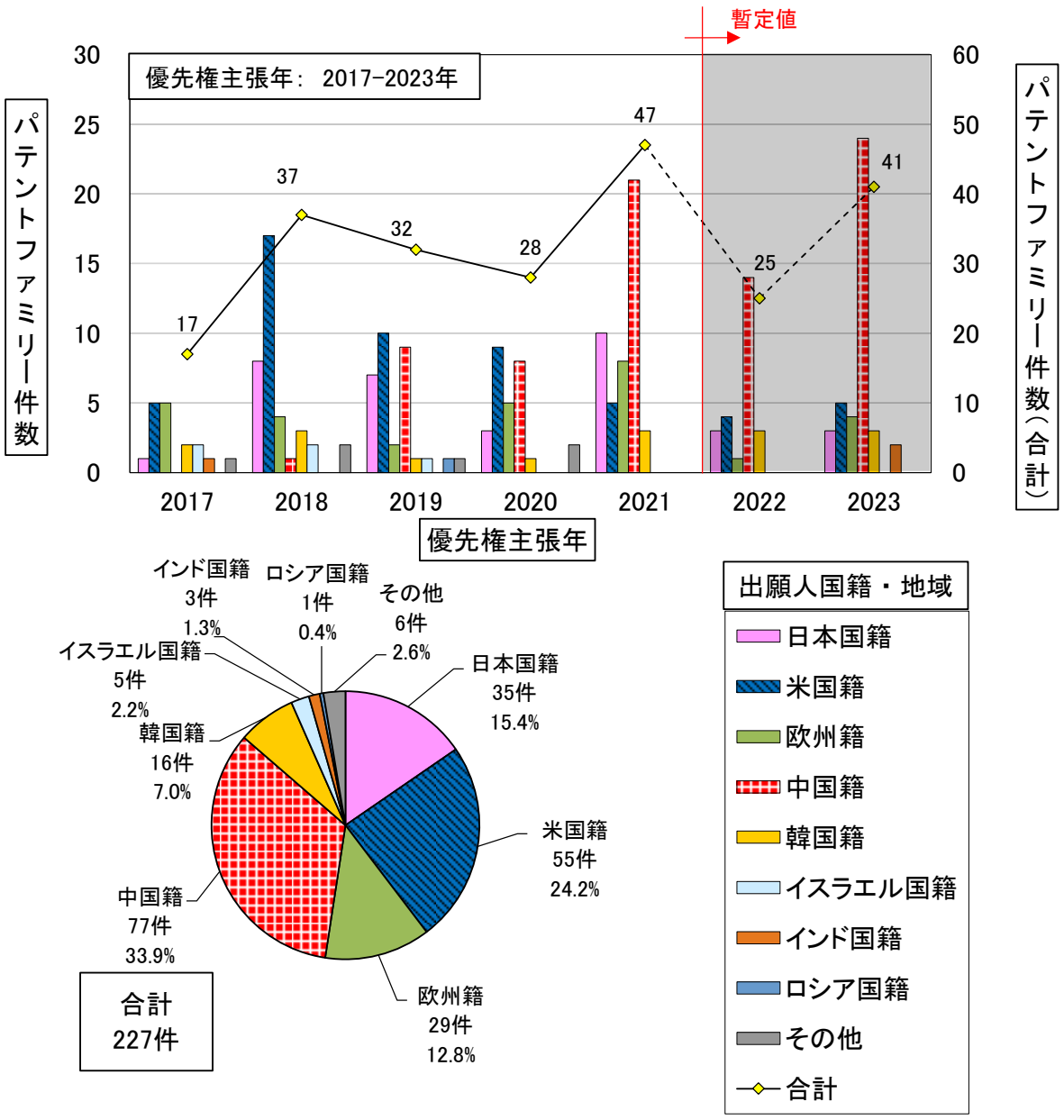
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-5　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝製造）



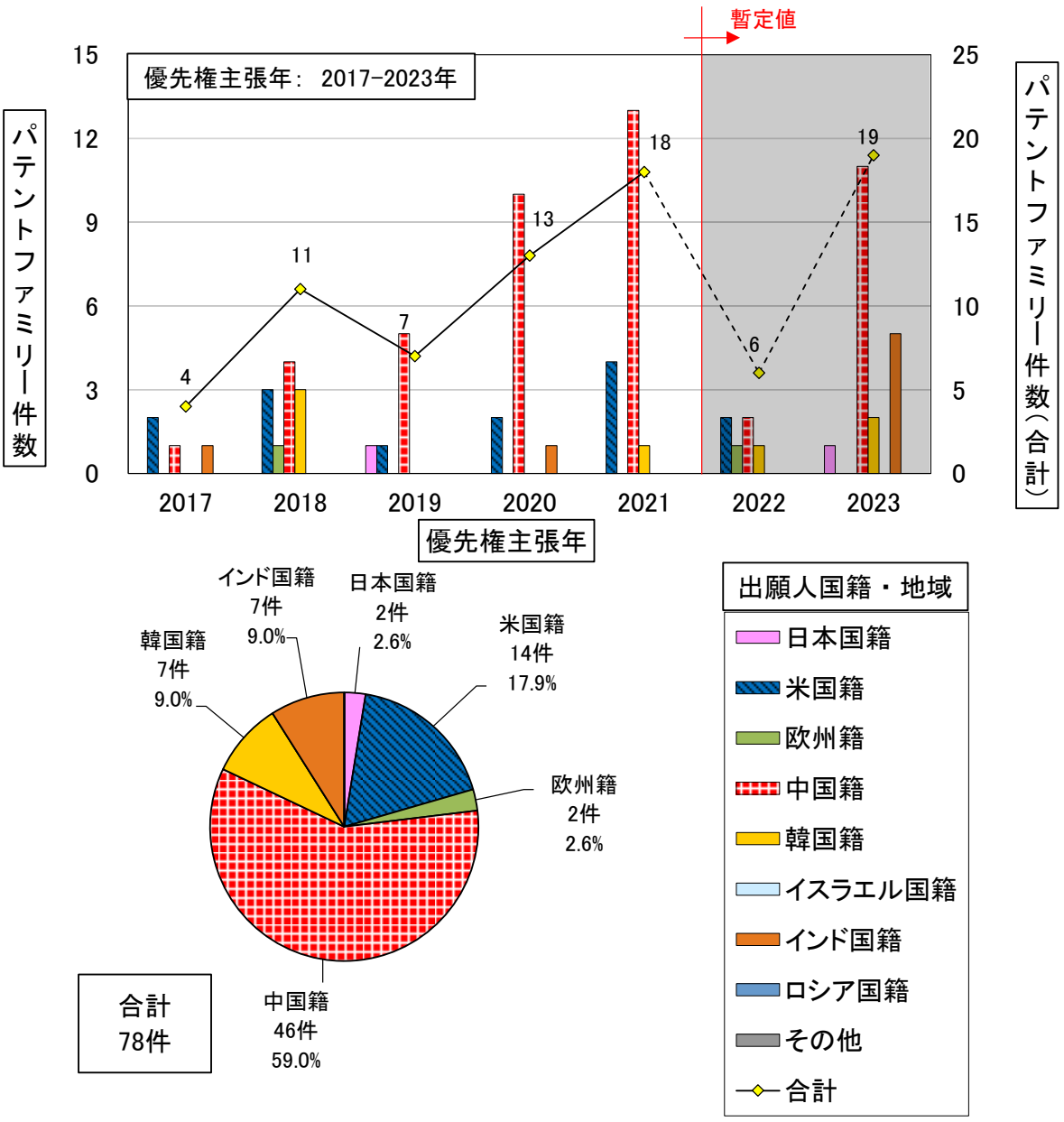
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-6　出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝交通システム）



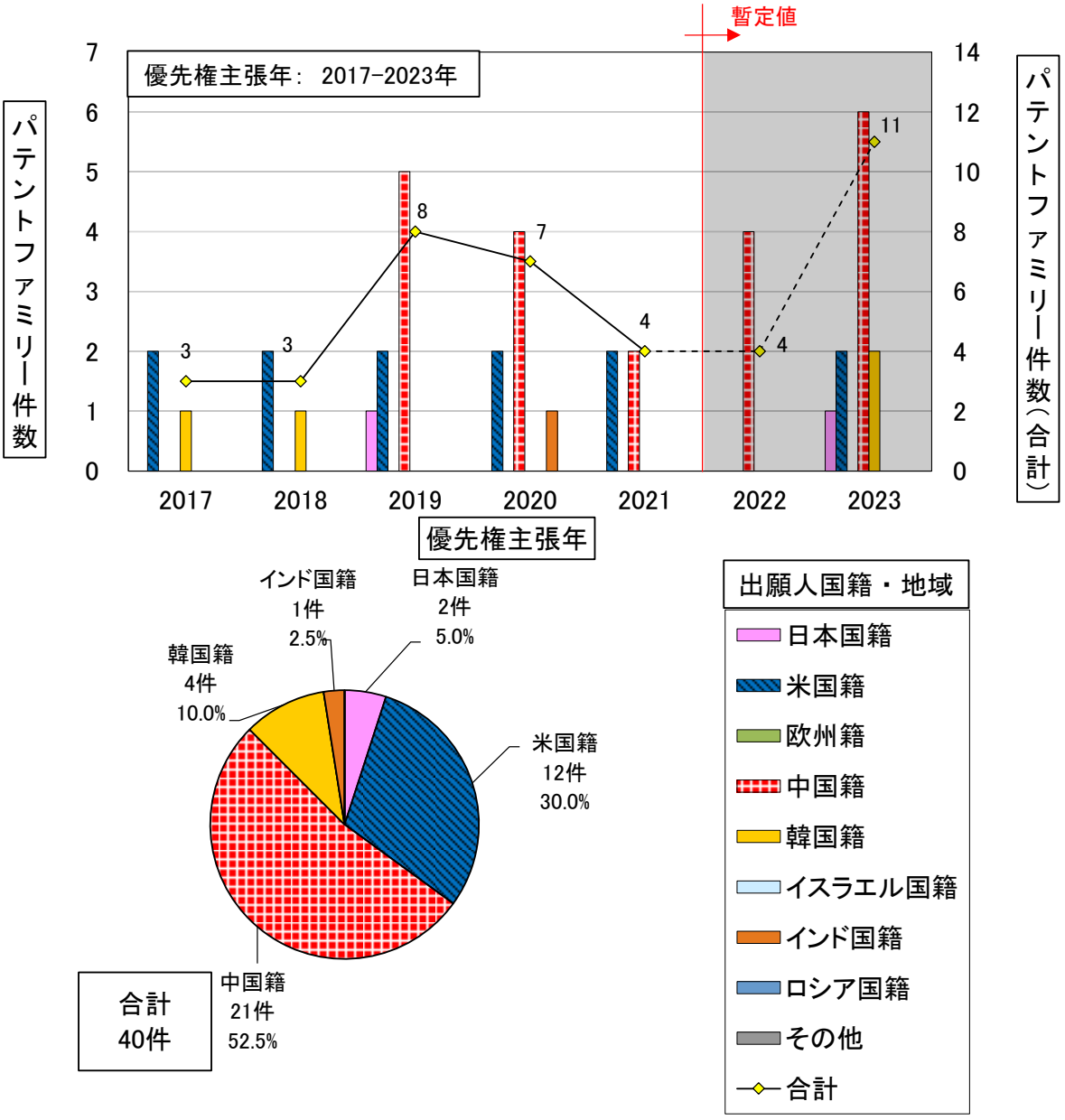
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-7　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝教育）



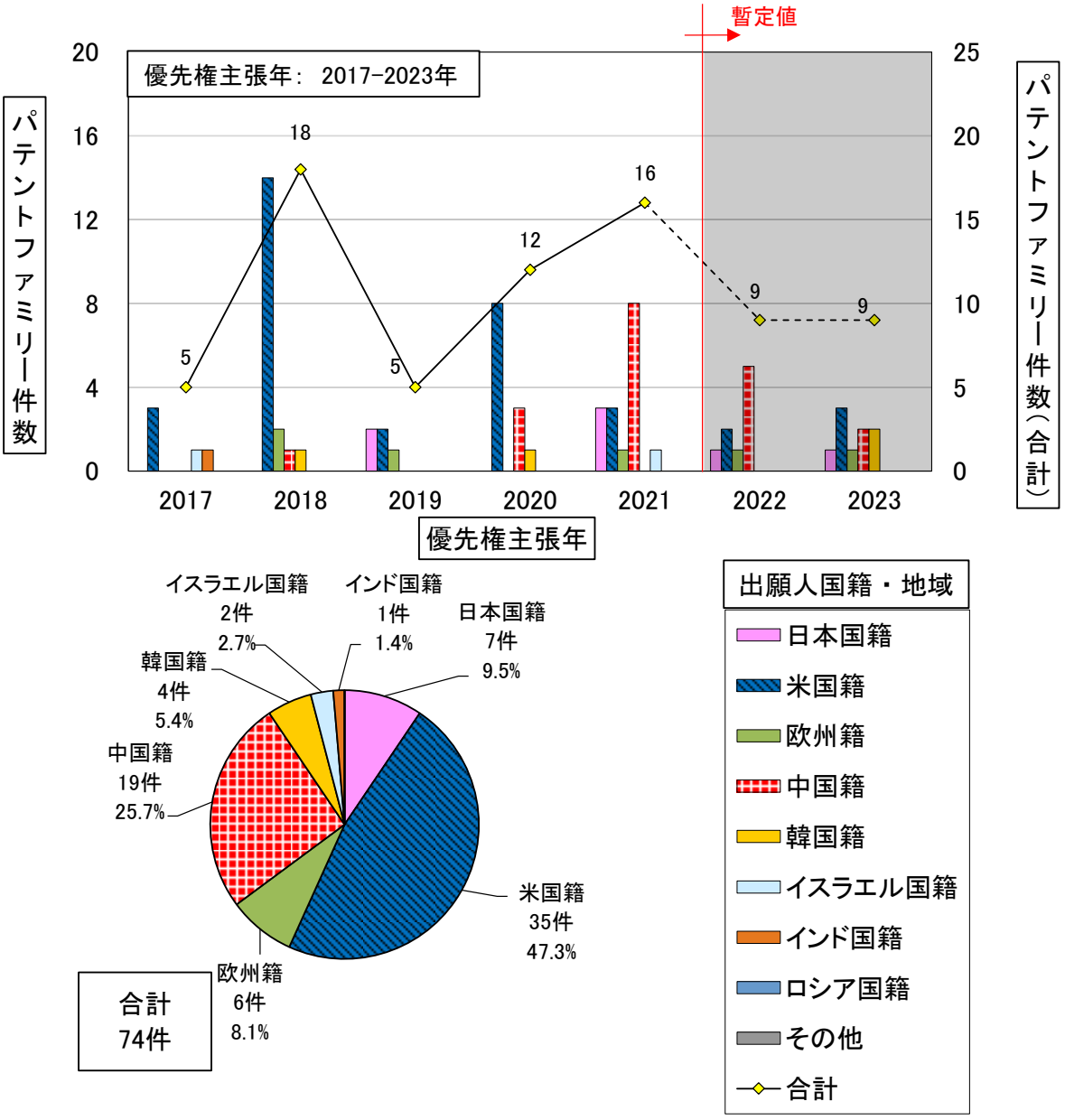
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-8　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝学術研究）



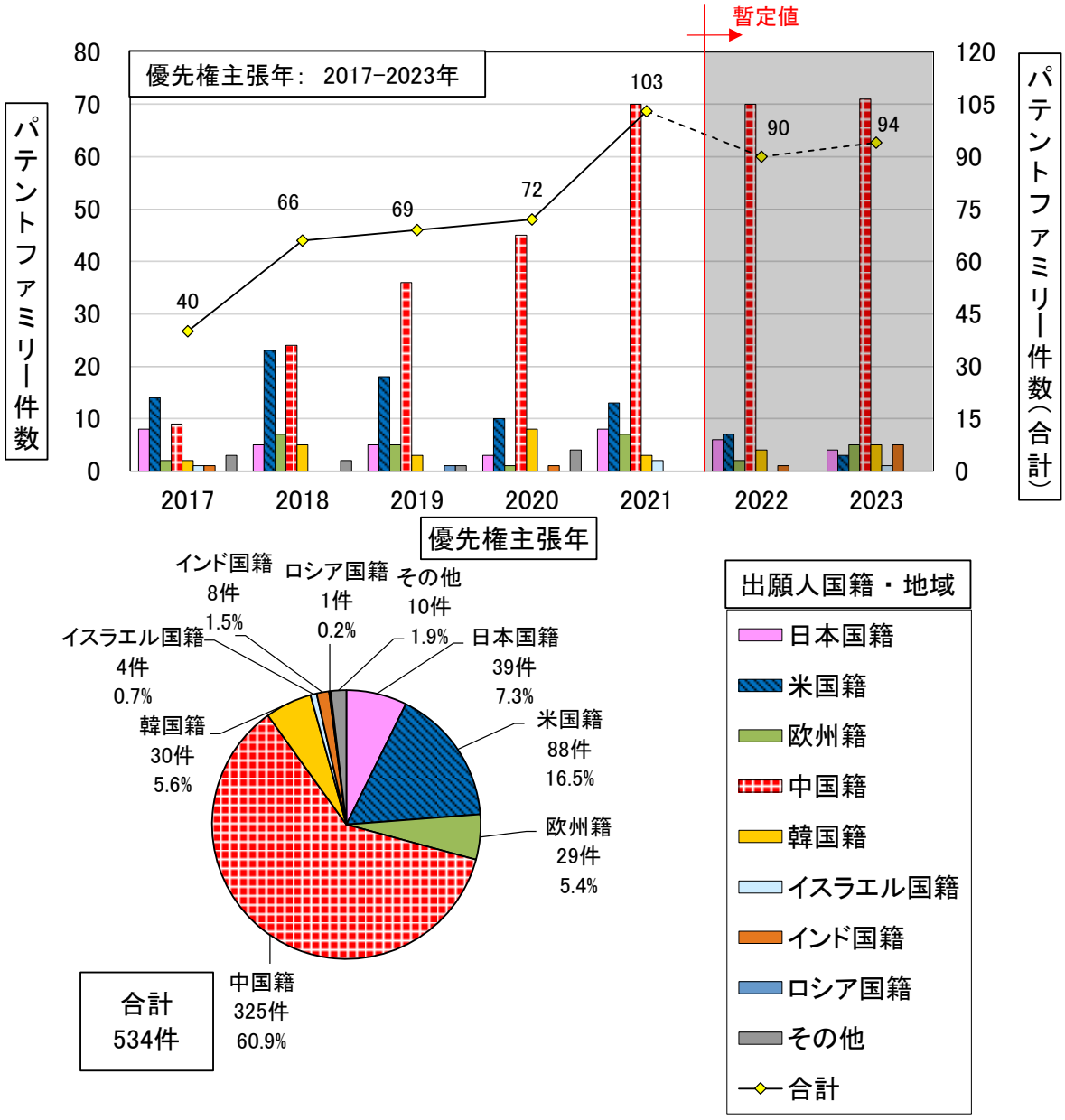
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-9　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝物流）



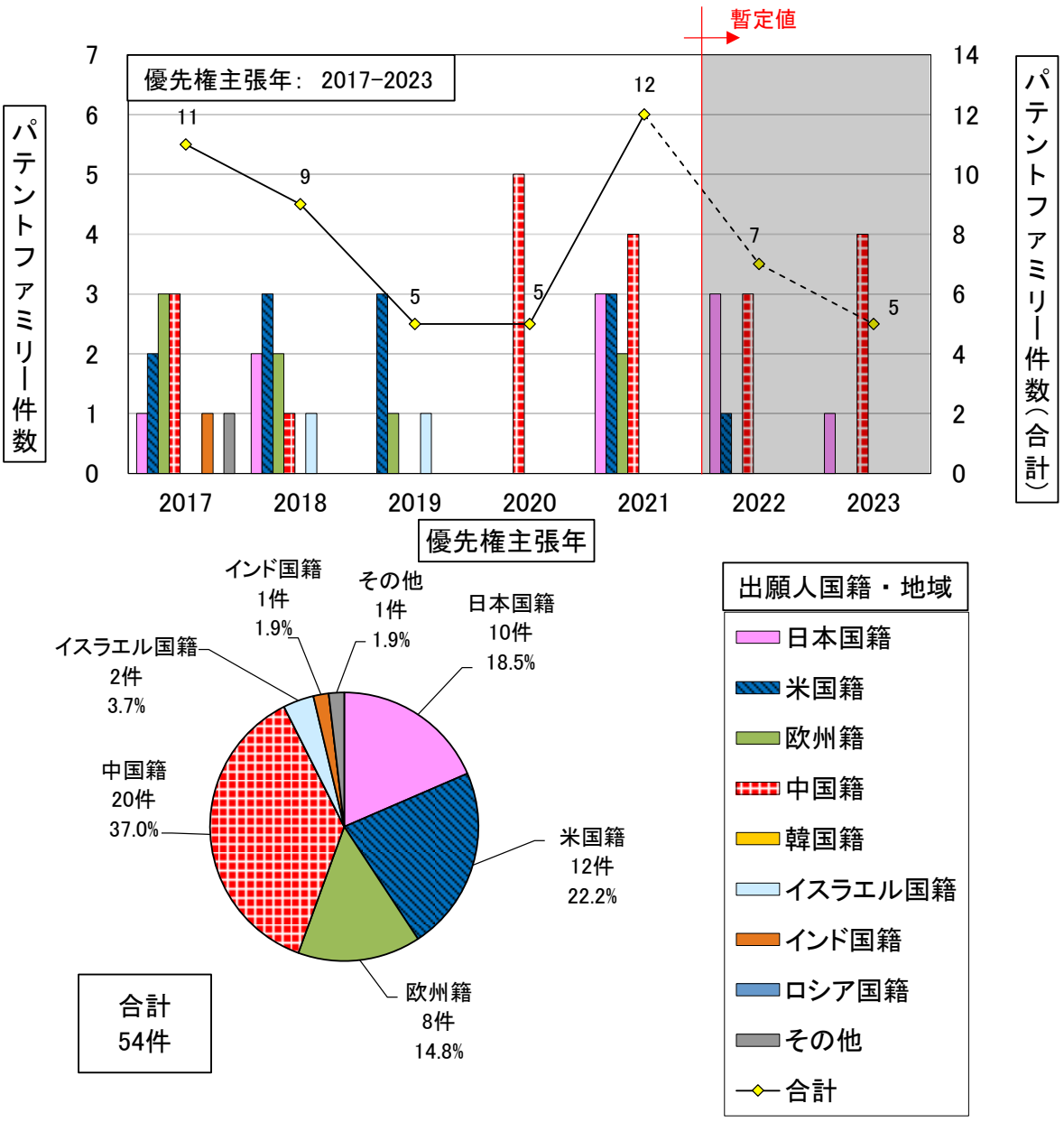
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-10　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝電力）



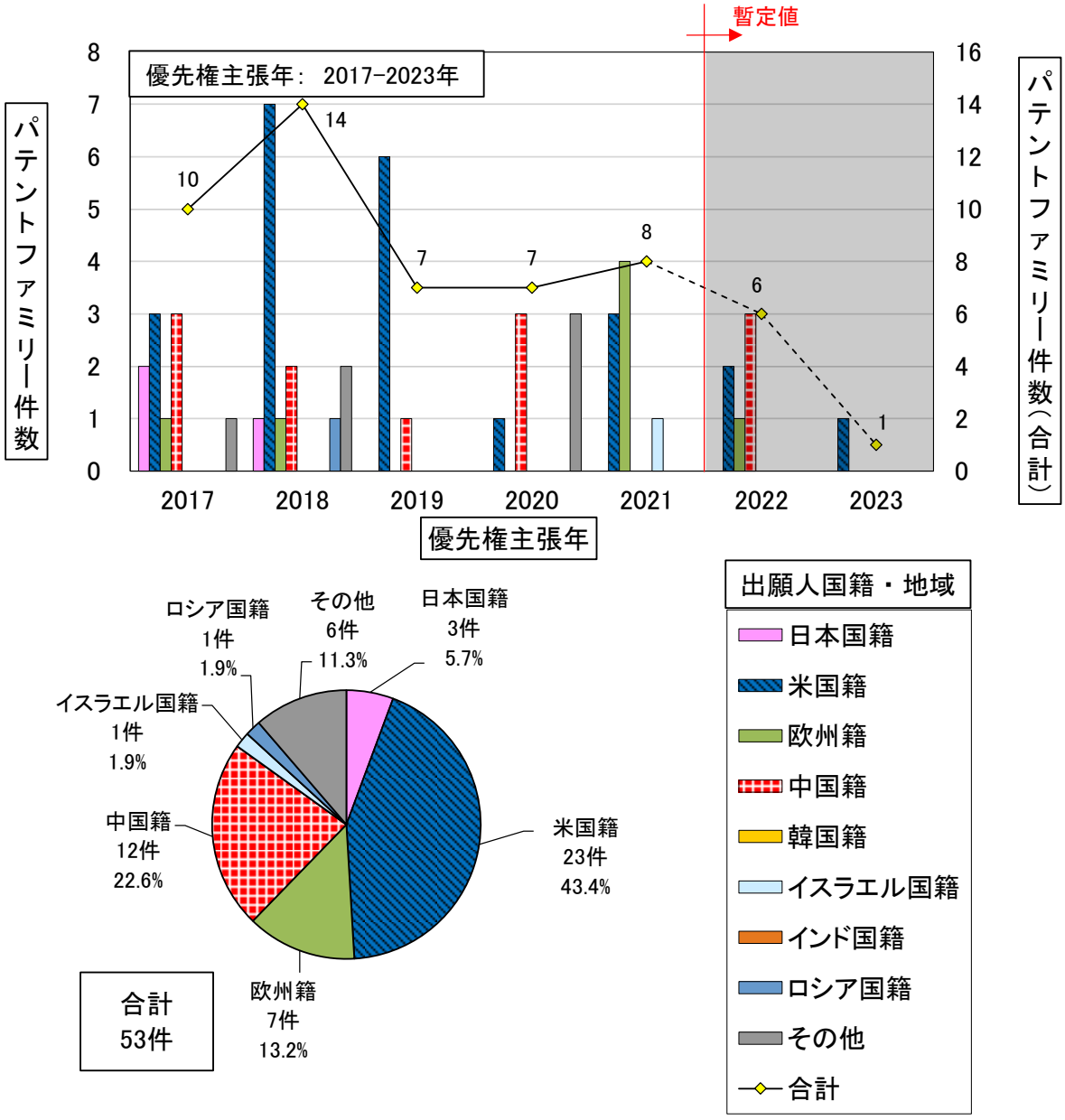
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-11　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝鉄道）



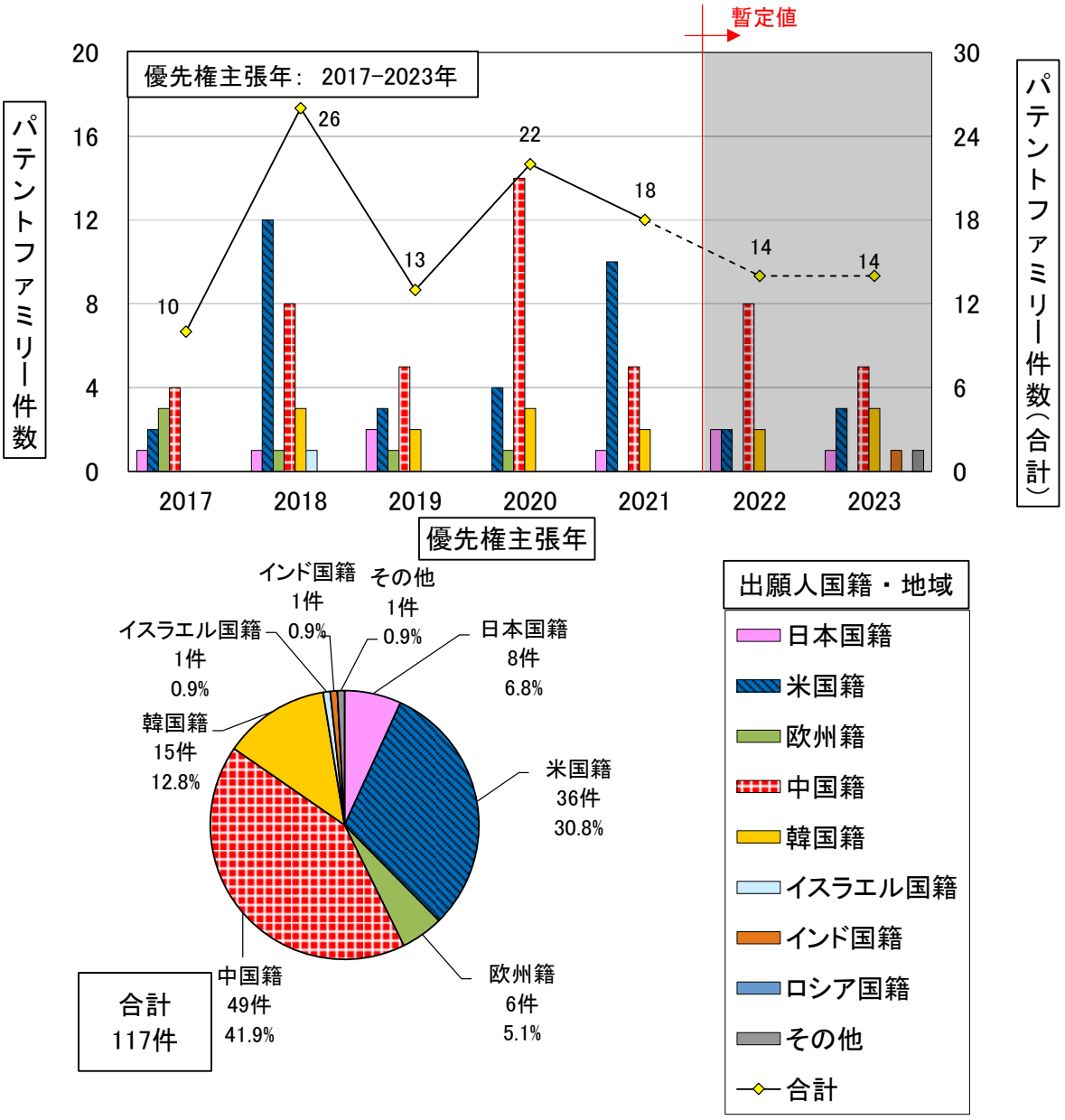
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-12　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝石油）



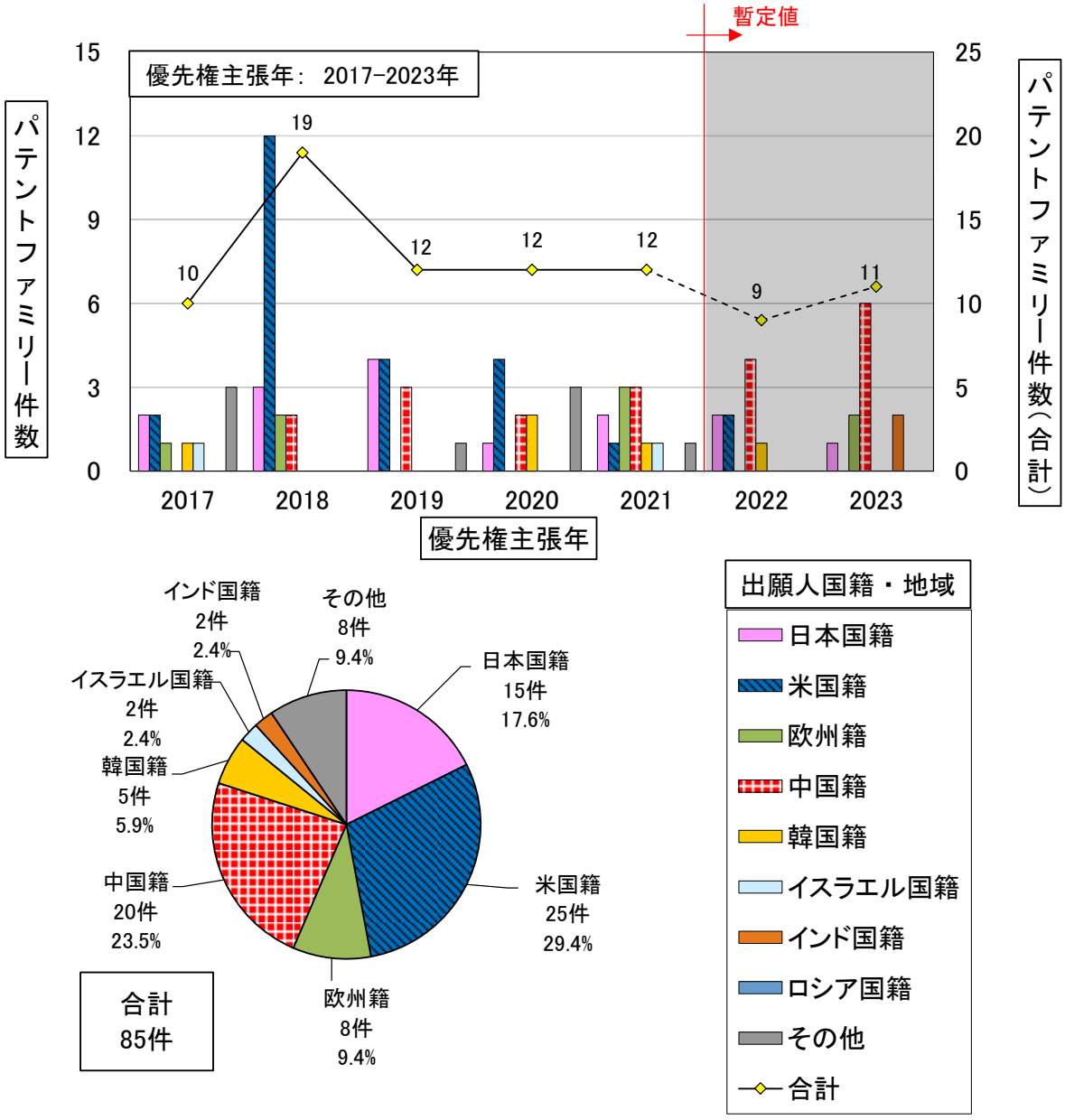
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-13　出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝政府・行政サービス）



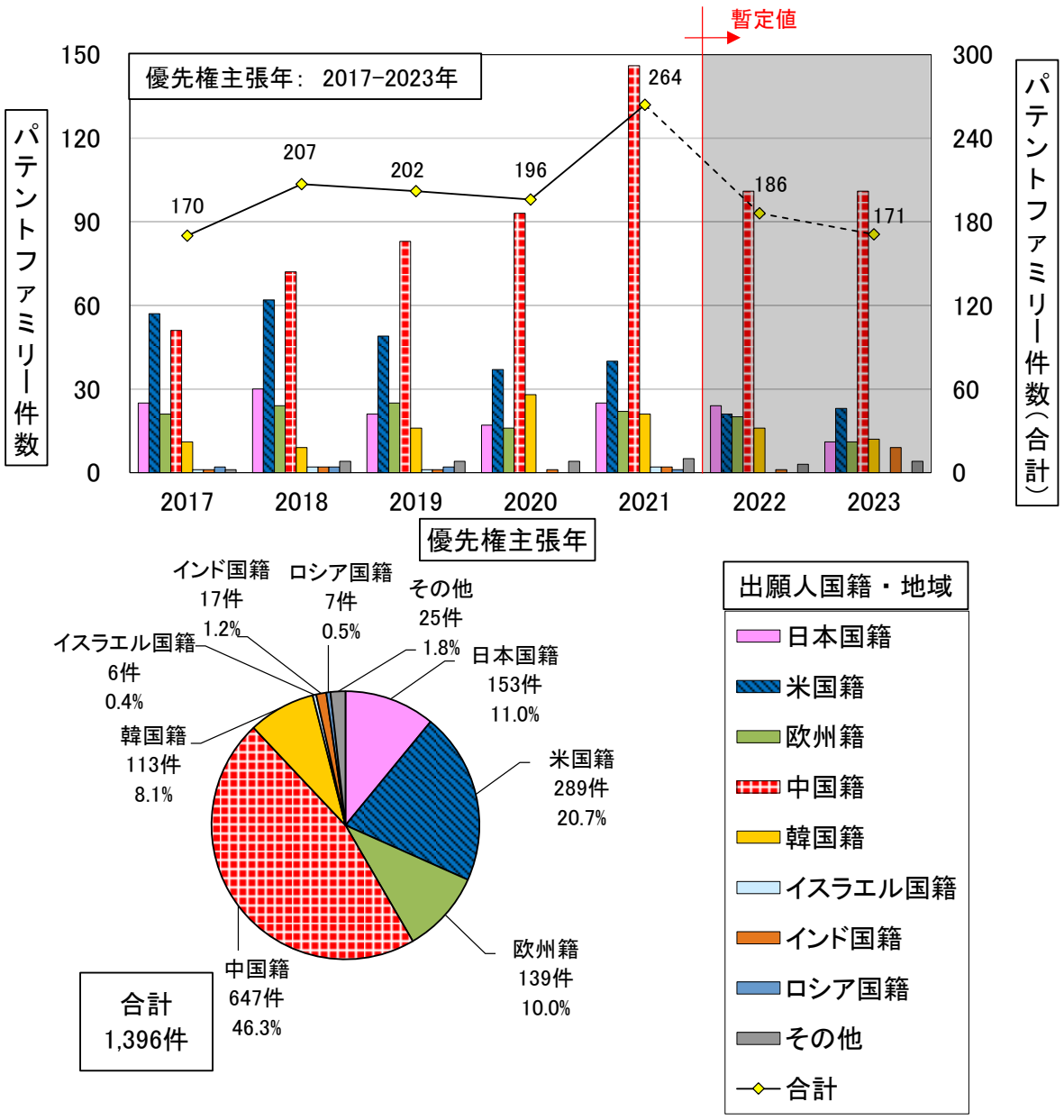
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-14　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別]　パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝水道）



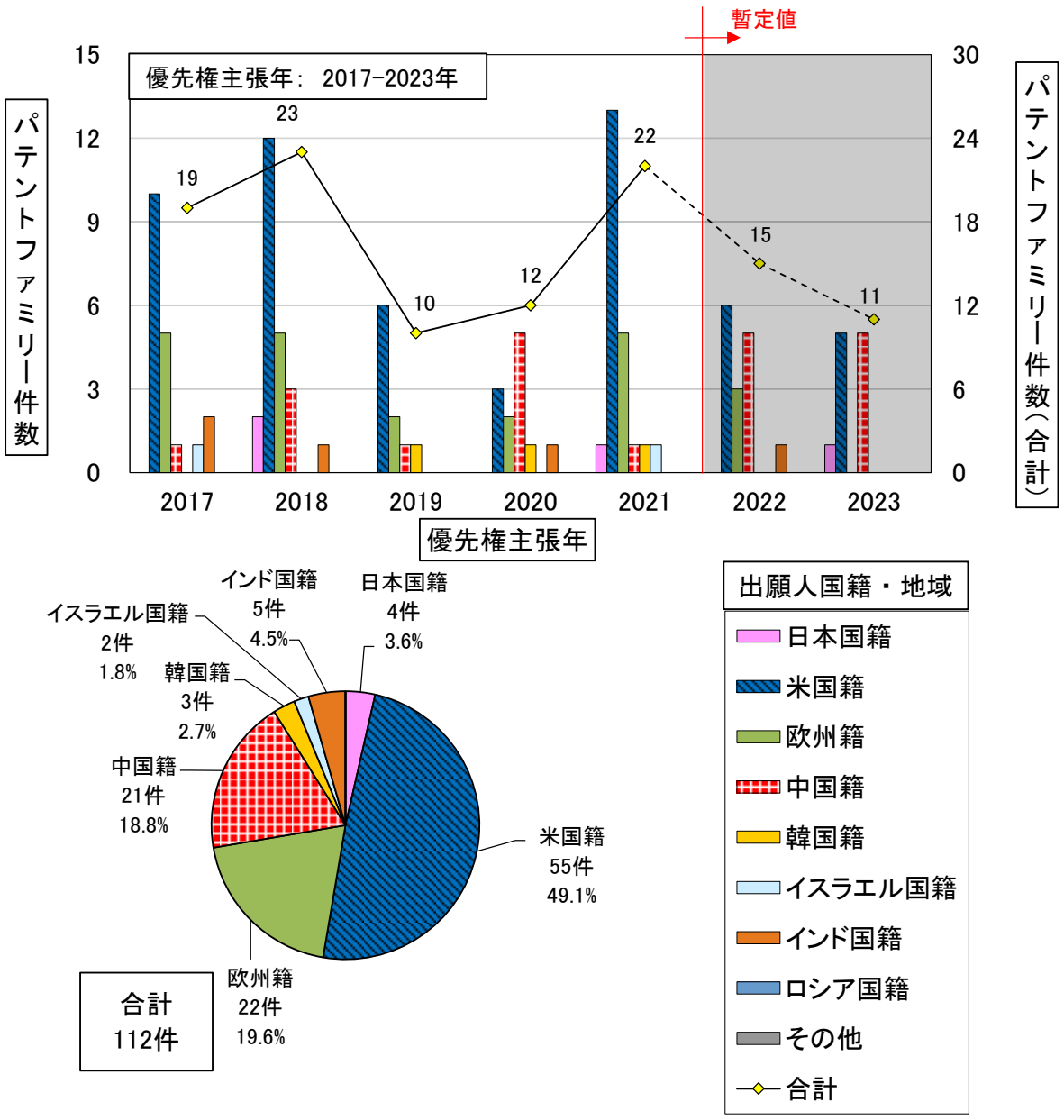
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-15　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝情報通信）



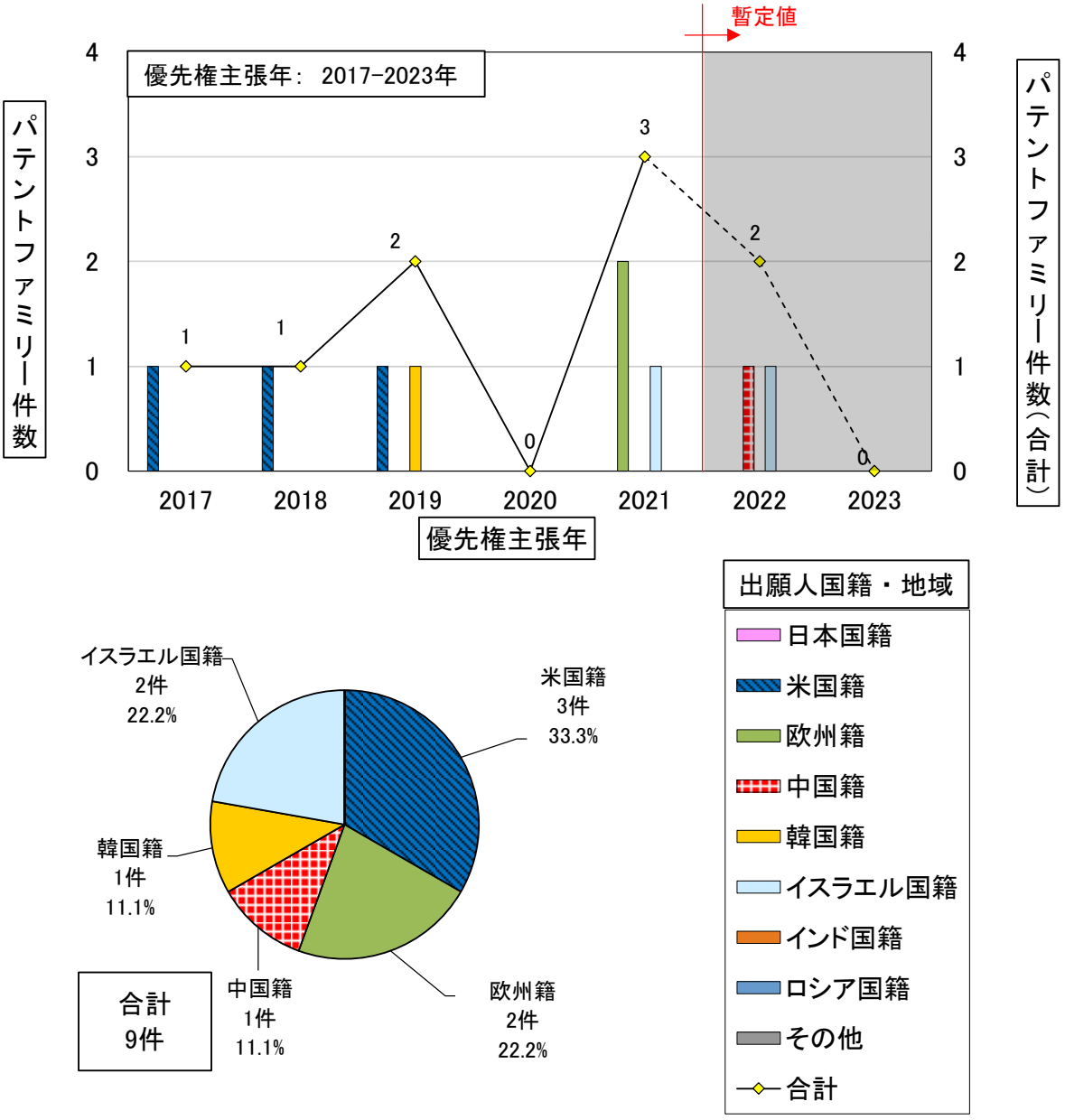
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-16　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝航空）



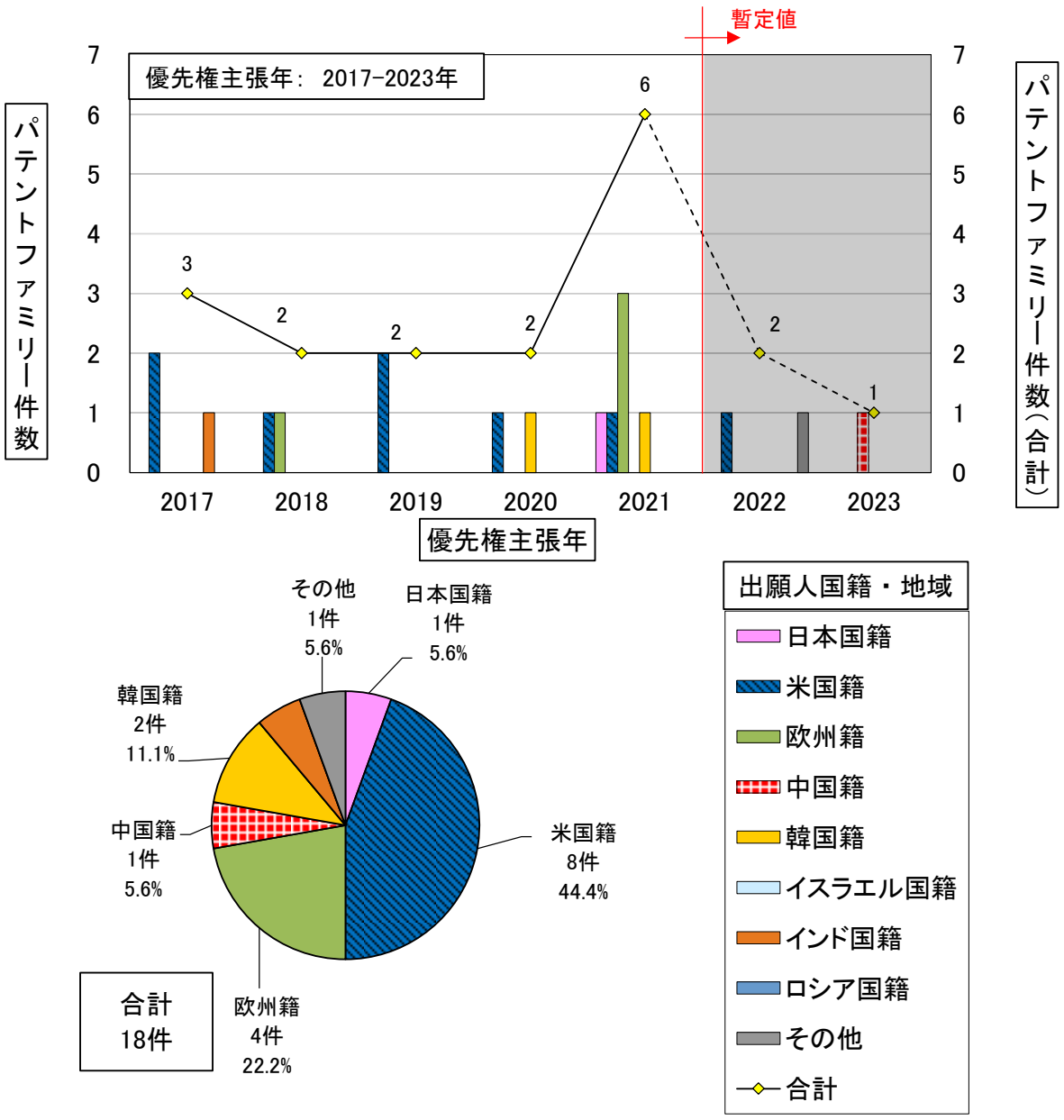
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-17　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝港湾）



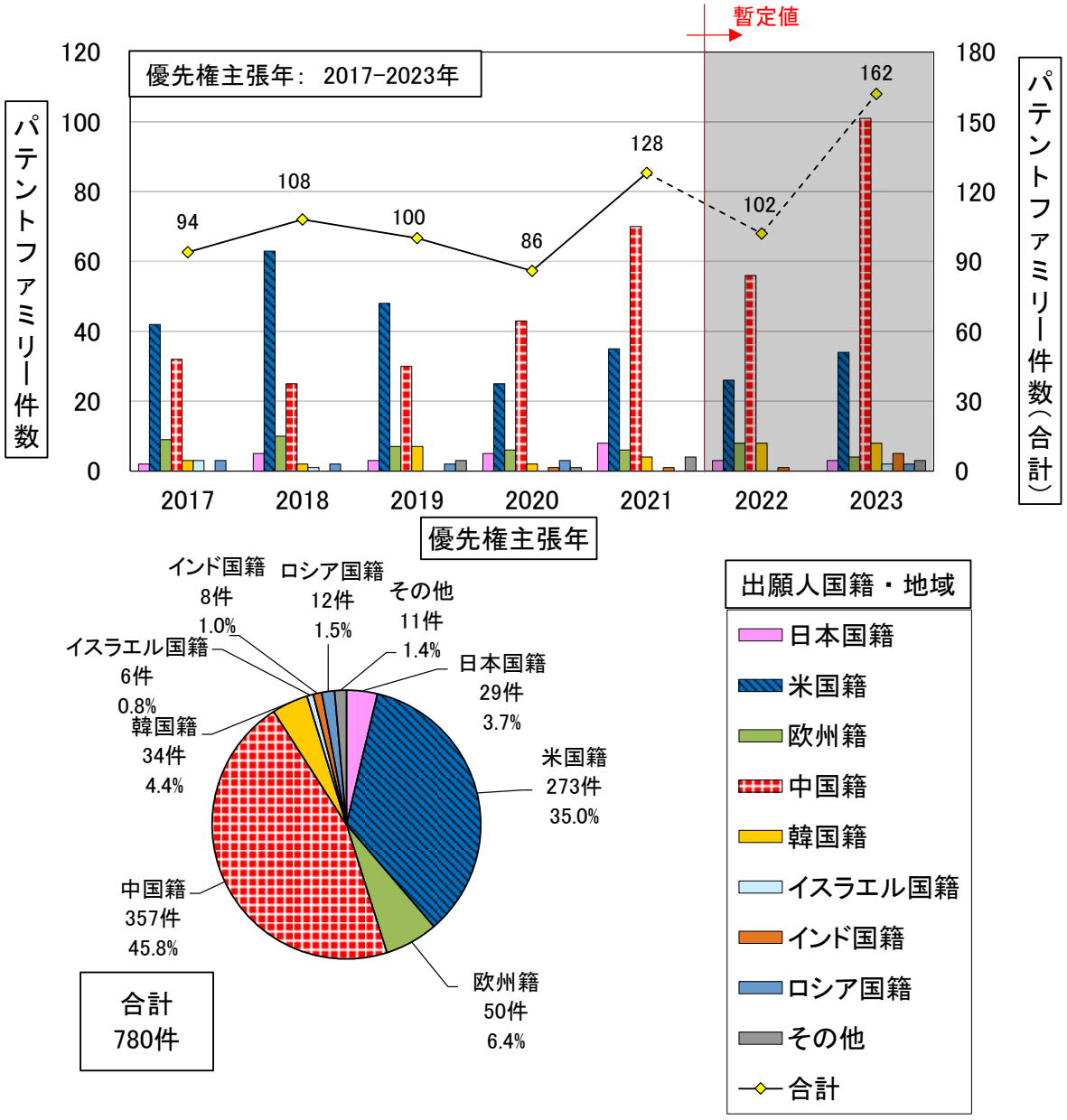
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-18　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝空港）



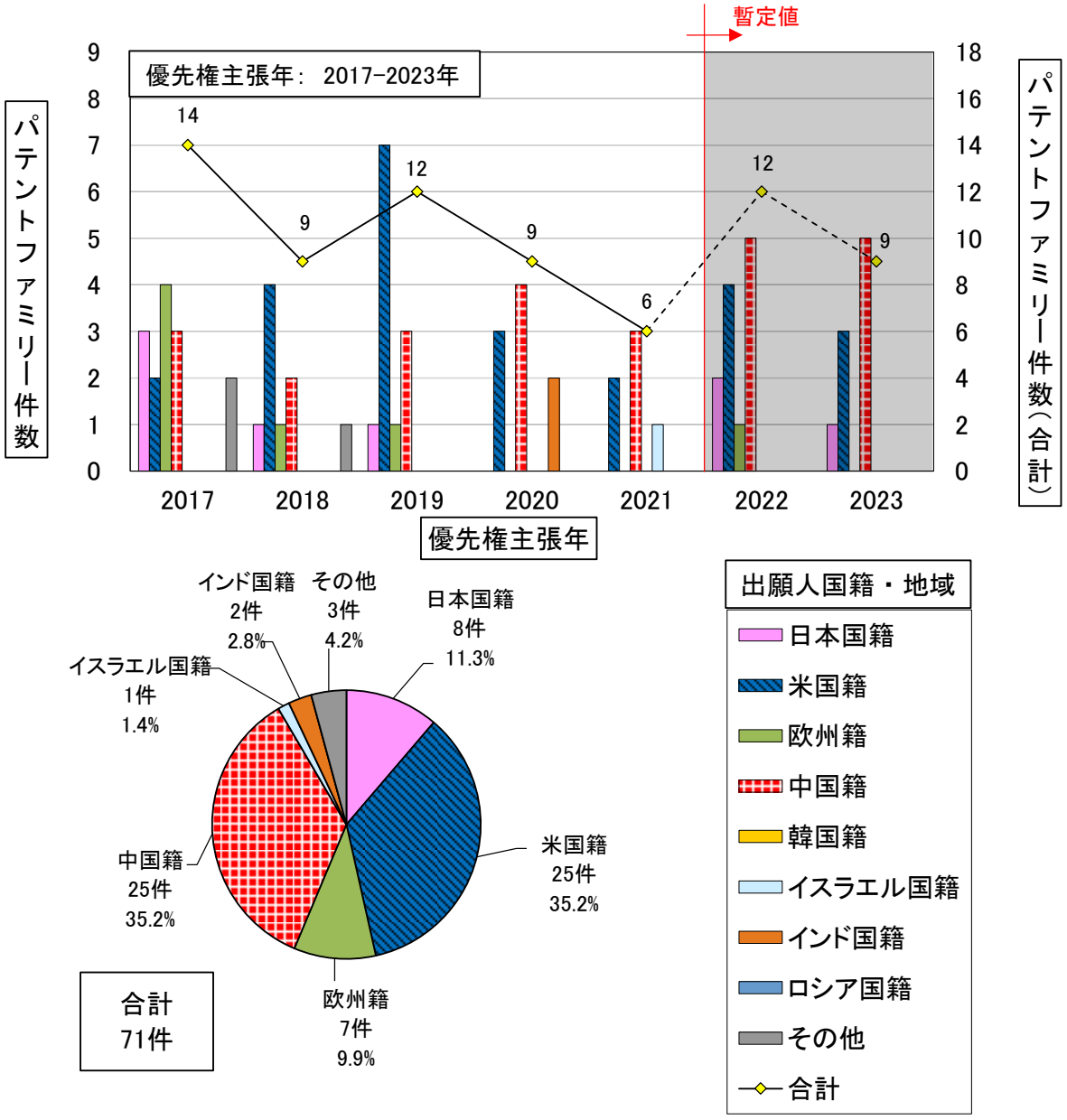
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-19　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝金融）



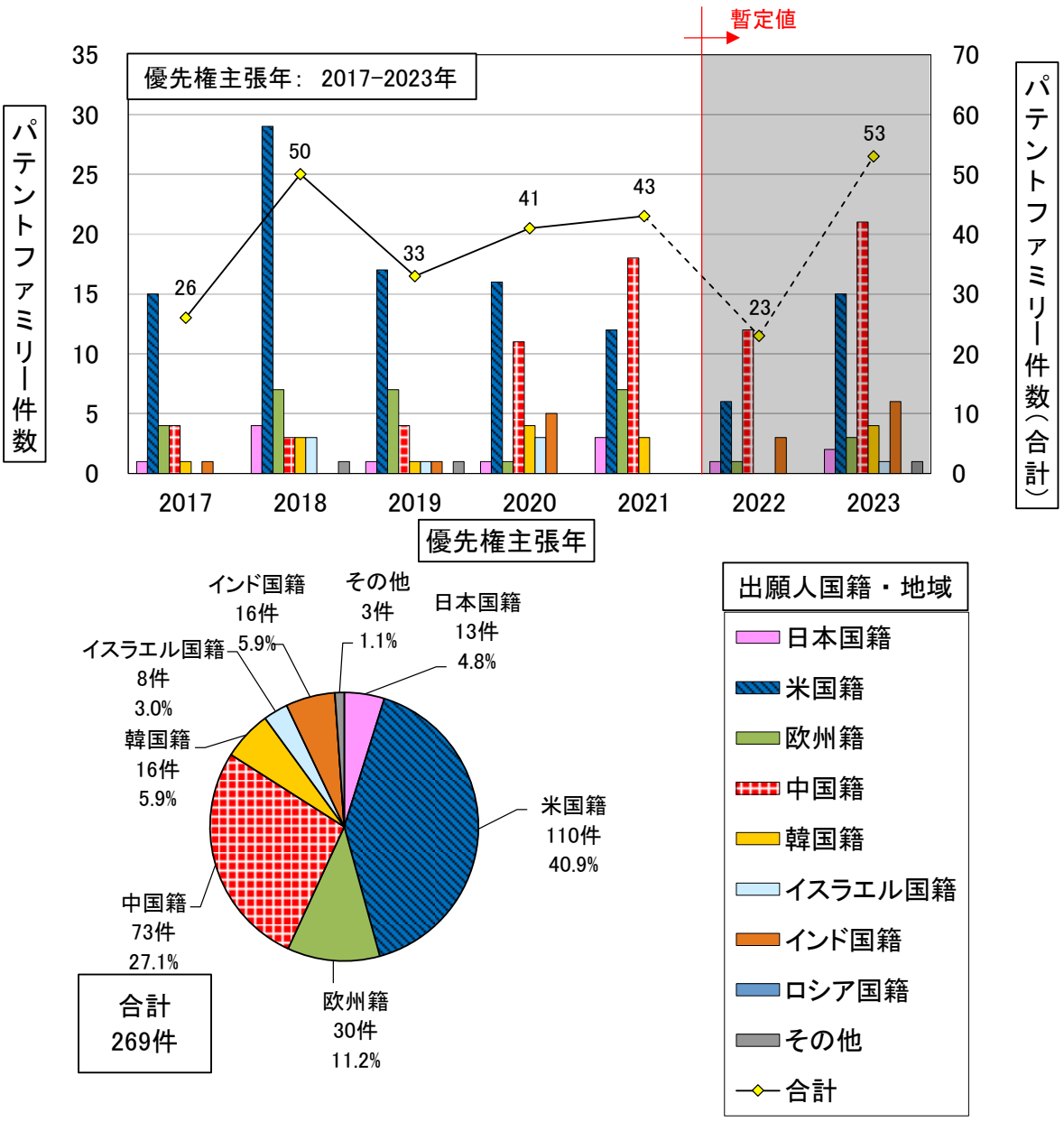
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-20　［出願先：日米欧中韓以印露 WO］［技術区分別］［出願人国籍・地域別］パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝化学）



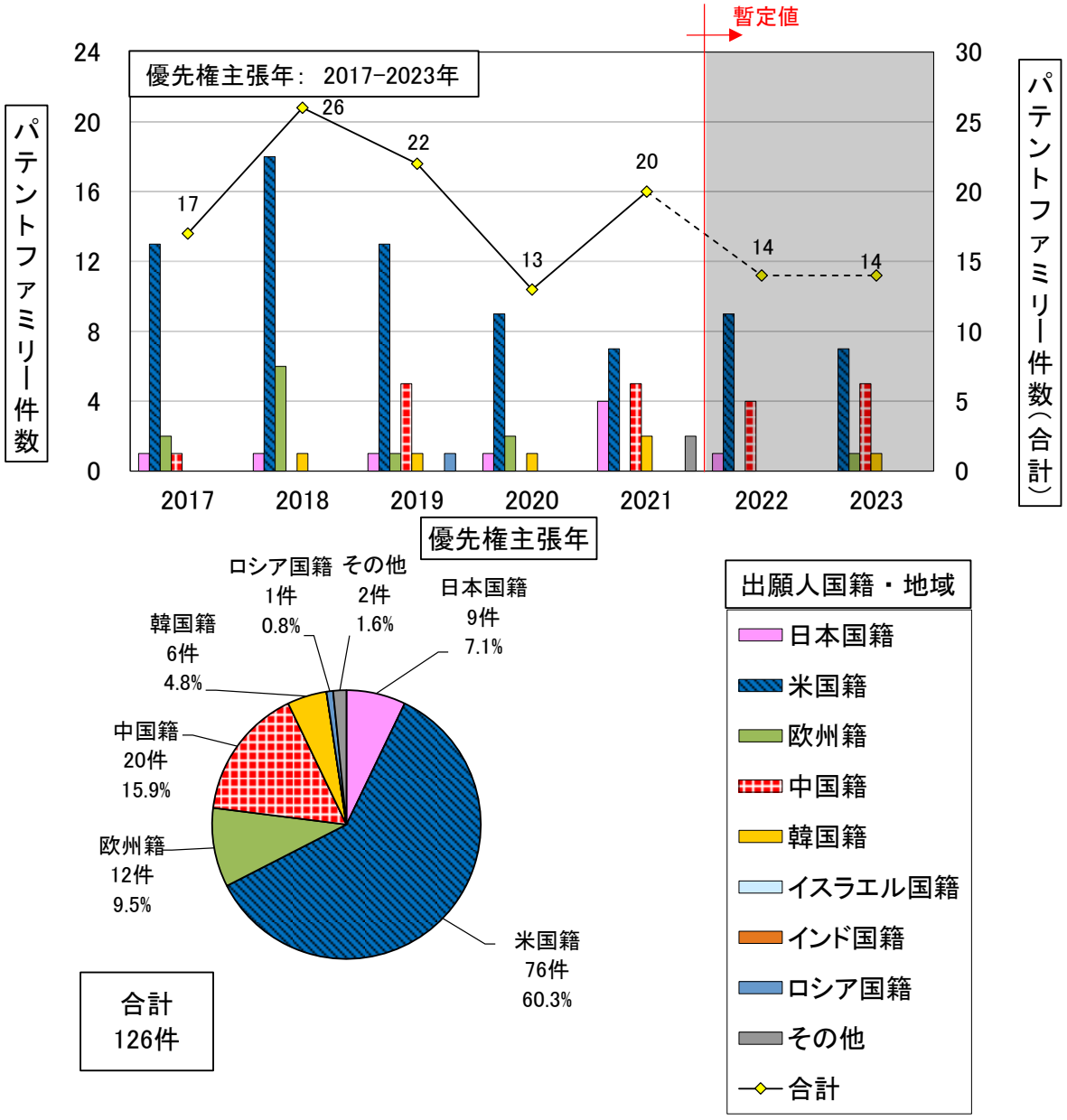
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-21　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝医療）



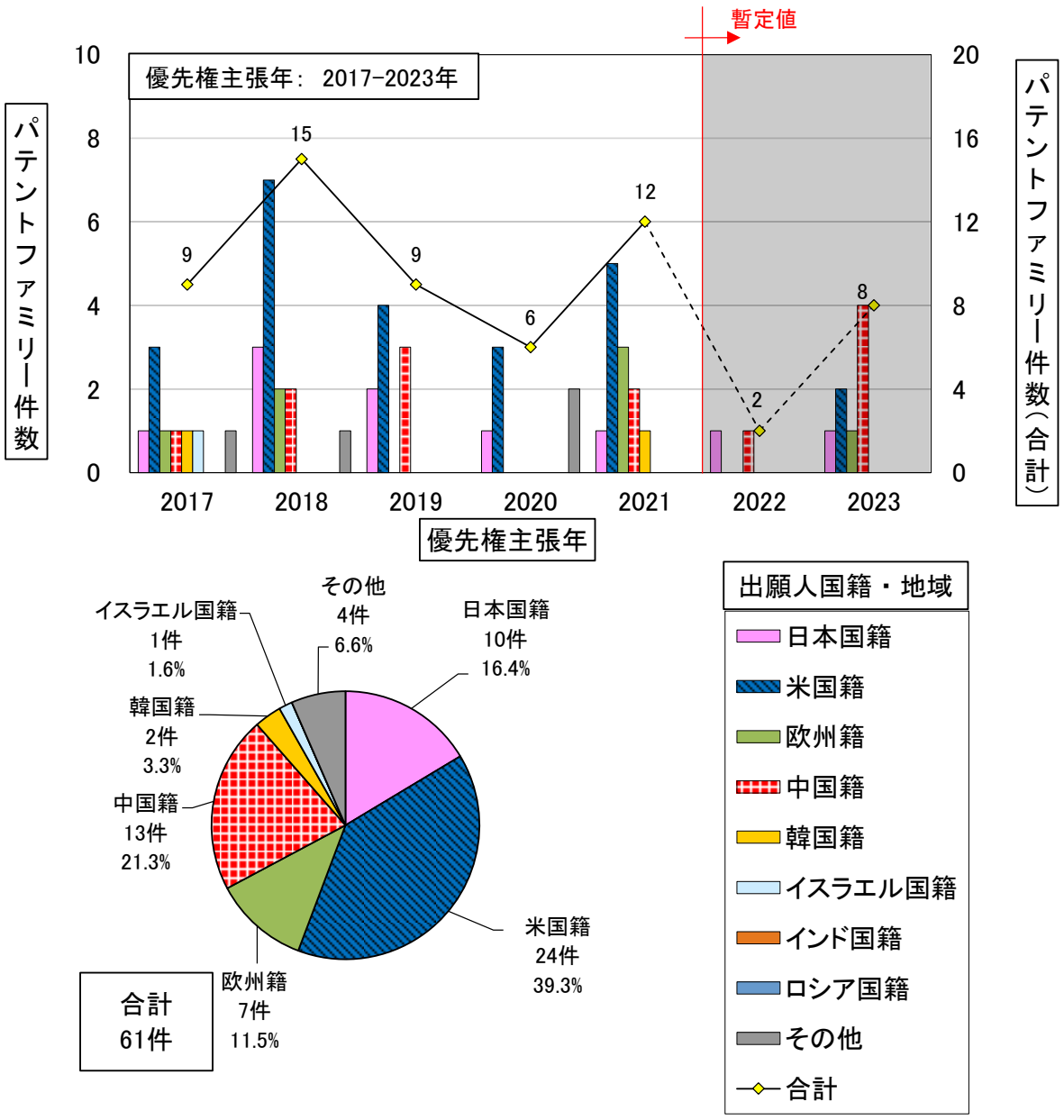
注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

図-参考-22　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝クレジット）



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

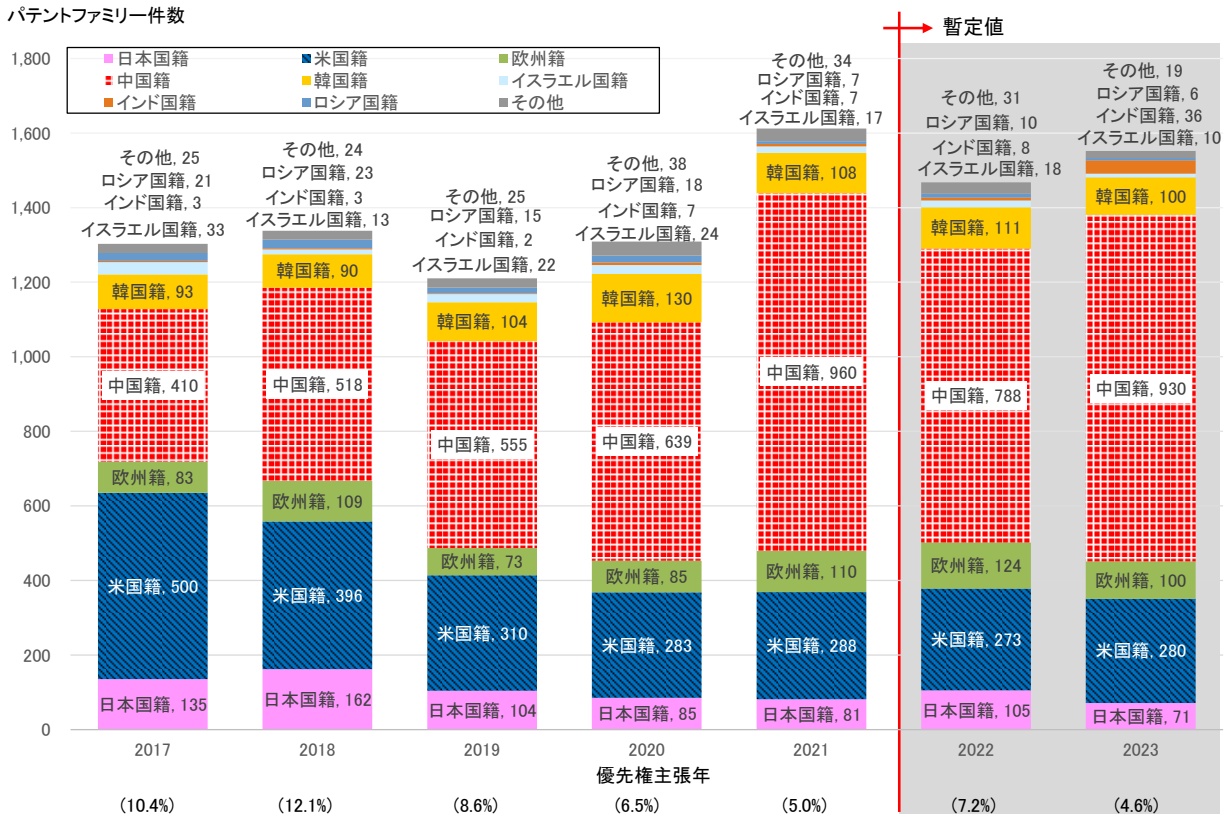
図-参考-23　[出願先：日米欧中韓以印露 WO][技術区分別][出願人国籍・地域別] パテントファミリー件数年次推移及びパテントファミリー件数比率（適用領域＝ガス）



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。

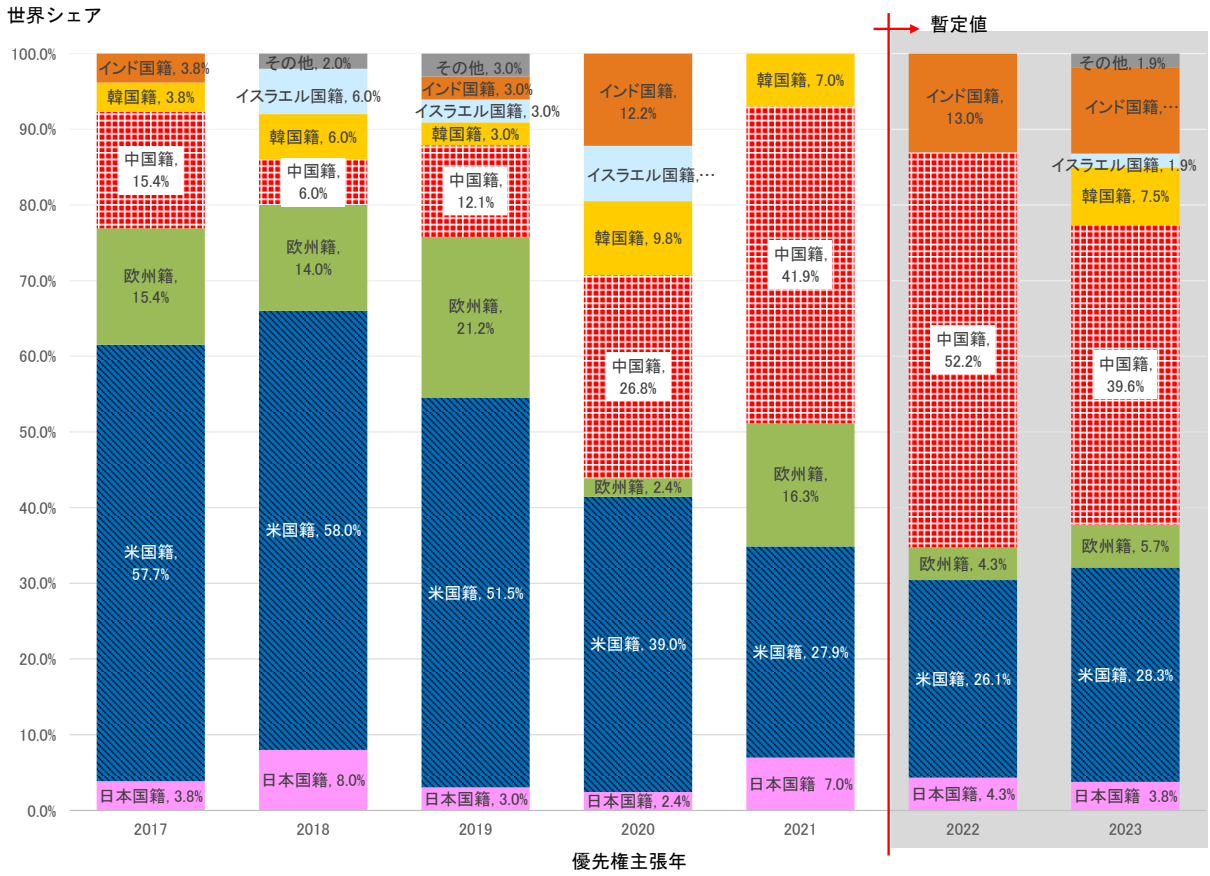
2． 総合分析に関する参考図表

図-参考-24 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数年次推移及び件数比率（脅威インテリジェンス）



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。
※括弧書きは日本国籍の割合を示す。
※本図は、表 4-4-2 の内容を可視化したものである。

図-参考-25 ［出願先：日米欧中韓以印露 WO］［出願人国籍・地域別］パテントファミリー件数比率の年次推移（医療）



注）2022 年以降はデータベース収録の遅れ、PCT 出願の各国以降のずれ等で全出願データを反映していない可能性がある。
※本図は、表 4-4-11 の内容を可視化したものである。

令和７年度特許出願技術動向調査
－サイバー攻撃検知技術～不正侵入・マルウェア等の検知に向けた情報セキュリティ技術～－
アドバイザリーボード名簿

（敬称略、所属・役職等は令和８年２月現在）

委員長

松本　勉	国立研究開発法人産業技術総合研究所　フェロー
	国立大学法人横浜国立大学先端科学高等研究院　上席特別教授

委員

鵜飼　裕司	株式会社 FFRI セキュリティ　代表取締役社長
大久保　隆夫	学校法人岩崎学園情報セキュリティ大学院大学
	情報セキュリティ研究科長・教授
笠間　貴弘	国立研究開発法人情報通信研究機構
	サイバーセキュリティ研究所　サイバーセキュリティ研究室　室長
森井　昌克	国立大学法人神戸大学大学院　名誉教授・特命教授

＊委員は五十音順に記載

特許庁オブザーバ

宮田　繁仁	特許庁　審査第四部　情報処理　上席審査長
濵中　信行	特許庁　審査第四部　情報処理(情報セキュリティ)　技術担当室長
岸野　徹	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
金沢　史明	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
川原　光司	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
上島　拓也	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
加藤　優一	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
栁谷　侑	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
酒井　大門	特許庁　審査第四部　情報処理(情報セキュリティ)　審査官
吉倉　大智	特許庁　審査第四部　審査調査室　副査
中村　俊之	特許庁　総務部　企画調査課　知財動向班　知財動向班長
馬場　亮人	特許庁　総務部　企画調査課　知財動向班　知財動向班長（前任）
温井　脩市	特許庁　総務部　企画調査課　知財動向班　技術動向係長
井上　瞳	特許庁　総務部　企画調査課　知財動向班　技術動向係員
松田　恭典	特許庁　総務部　企画調査課　知財動向班　工業所有権調査員

その他オブザーバ

石坂　知樹	経済産業省　商務情報政策局　サイバーセキュリティ課　課長補佐
長谷川　智宏	経済産業省　商務情報政策局　サイバーセキュリティ課　係長
横井　一仁	国立研究開発法人新エネルギー・産業技術総合開発機構 イノベーション戦略センター　デジタルユニット　ユニット長
大杉　伸也	国立研究開発法人新エネルギー・産業技術総合開発機構 イノベーション戦略センター　デジタルユニット　上席研究員
秋葉　拓也	国立研究開発法人新エネルギー・産業技術総合開発機構 イノベーション戦略センター　デジタルユニット　上席研究員
中村　隆顕	国立研究開発法人新エネルギー・産業技術総合開発機構 イノベーション戦略センター　デジタルユニット　主任研究員
瀧澤　剛	国立研究開発法人新エネルギー・産業技術総合開発機構 半導体・情報インフラ部　チーム長
田中　俊博	国立研究開発法人新エネルギー・産業技術総合開発機構 半導体・情報インフラ部　専門調査員
卯川　正隆	国立研究開発法人新エネルギー・産業技術総合開発機構 半導体・情報インフラ部　専門調査員
神市　章二	国立研究開発法人新エネルギー・産業技術総合開発機構 半導体・情報インフラ部　主査
杉浦　守	国立研究開発法人新エネルギー・産業技術総合開発機構 半導体・情報インフラ部　専門調査員
西潟　久美子	国立研究開発法人新エネルギー・産業技術総合開発機構 バイオ・材料部　チーム長
髙橋　遥	国立研究開発法人新エネルギー・産業技術総合開発機構 バイオ・材料部　主任
伊藤　孝一	国立研究開発法人新エネルギー・産業技術総合開発機構 航空・宇宙部　主査
平野　潤也	国立研究開発法人新エネルギー・産業技術総合開発機構 航空・宇宙部　主査
山本　研吾	国立研究開発法人新エネルギー・産業技術総合開発機構 航空・宇宙部　主査
森　健吾	国立研究開発法人新エネルギー・産業技術総合開発機構 航空・宇宙部　主査
松坂　志	独立行政法人情報処理推進機構セキュリティセンター 早期警戒担当副部長

○本調査の実施と報告書の作成に当たっては、本調査のために設置された上記委員から構成されるアドバイザリーボードの助言を活用した。
○知財データ分析に当たっては、野崎篤志氏（株式会社イーパテント 代表取締役社長）から助言をいただいた。

非　売　品
禁無断転載

令和７年度特許出願技術動向調査
－サイバー攻撃検知技術～不正侵入・マルウェア
等の検知に向けた情報セキュリティ技術～－
令和８年３月

発行者　　特　許　庁
〒100-8915　東京都千代田区霞が関３－４－３
電　話　　０３－３５８１－１１０１（代表）

請負先　　NTT アドバンステクノロジ株式会社

乱丁、落丁がございましたら、上記までご連絡下さい