平成２７年度
特許出願技術動向調査報告書（概要）

情報セキュリティ技術

平成２８年２月

特　　許　　庁

問い合わせ先
特許庁総務部企画調査課 知財動向班
電話：０３－３５８１－１１０１（内線２１５５）

第１章　特許出願技術動向調査の目的

日本の情報セキュリティ技術関連市場で流通している製品・ツールの多くが、海外企業によって提供されている。サイバーセキュリティ上の脅威・リスクが急速に増大している海外では、国防のために開発された情報セキュリティ技術が民間に転用されていること、こうした技術を保有する海外企業が流通力のある日本の商社、ベンダー等と提携し、日本市場の開拓に力を入れていることが背景にある。また、海外では、自国の企業が研究開発で成果を出した情報セキュリティ技術を政府調達において採用することや、スタートアップ支援の充実や海外プロモーションの強化等を通じて情報セキュリティ分野の自国ベンチャーを育成することに積極的であり、その結果として、技術競争力を有する革新的な製品・ツールを持つ企業が輩出されているのに対し、日本では、海外と同様のスキームが必ずしも十分確立されているとは言えない状況であり、このことが国内技術や国内製品・ツールの競争構造に少なからぬ影響を与えている。

こうした状況のもと、情報セキュリティ分野に携わる日本企業において、大きな投資リスクを伴う革新的な製品・ツールの技術開発・研究開発を軽視する姿勢が強まってきている。海外企業から革新的な製品・ツールを調達して、それを既存製品に組み込むことで付加価値を高めて販売したり、国内の販売代理店となって、海外企業から手数料収入を得るなどのビジネスが収益を生み出しやすいことが認識されるようになってきている。このため、このままでは国内技術や国内製品・ツールの開発力低下は避けられない状況であり、情報セキュリティ分野のコアとなる製品・ツールが海外製品・ツールとなり、国家安全保障の機能強化や重要インフラの保護、日本が強みを持つ産業の国際競争力の更なる向上等に対して、情報セキュリティ技術の観点から適切な措置を講じることができなくなることが懸念される。

また、日本においては、東京都が 2020 年東京オリンピック・パラリンピック競技大会の開催都市となり注目を集めていることから、過去の大会と同様、今後、サイバー攻撃などの情報セキュリティに係る問題が各方面で顕在化することが予想されている。このため、2020 年東京オリンピック・パラリンピック競技大会開催に向けて、情報セキュリティ分野の技術等の開発の加速が必要であり、さらにこれをきっかけとして、革新的な技術等の開発や国産技術等の開発、情報セキュリティ産業の振興を含めた情報セキュリティ分野の技術開発戦略を中長期的な視点で検討し策定することが必要である。

本調査の目的は、上述の課題認識を踏まえ、今後の国家安全保障の機能強化や、日本が強みを持つ産業の国際競争力の更なる向上等といった観点を勘案し、日本企業が本来、技術競争力を保有しておくべき技術・製品・ツールの領域を、特許出願動向の分析により明らかにし、当該領域の今後の技術開発・研究開発の推進力向上に繋げることである。

また、上述の課題認識を踏まえて、本調査においては、以下についてもアウトプットを得るものとする。

・日本企業・政府機関が取り組むべき課題が何か
・今後目指すべき技術開発・研究開発の方向性が何か

第２章　調査対象技術範囲

第１節　調査対象技術

１．調査対象技術の概念

本調査では、調査対象の情報セキュリティ技術を、「侵入検知、ウイルス・マルウェア検知」、「ログ解析、リバースエンジニアリング」、「暗号技術」、「認証技術」の４つの技術分類で整理する。

侵入検知、ウイルス・マルウェア検知は、更に侵入検知とウイルス・マルウェア検知に分類できる。このうち、侵入検知は、不正アクセスや不正侵入に関わる手口と、不正アクセスや不正侵入を検知する際に収集される情報、対策としての予防・抑制、検知・判定手法、アクション等に言及する事項として定義する。また、アクションは、侵入を検知した後の対策として、アラート配信、警告、アクセス遮断、感染データ削除等に言及する事項として定義する。他方、ウイルス・マルウェア検知は、ウイルス、ワーム、トロイの木馬を含むマルウェアに関わる感染経路と、ウイルス、ワーム、トロイの木馬を含むマルウェアを検知する際に収集される情報、対策としての予防・抑制、検知・判定手法、アクション等に言及する事項として定義する。アクションについては、侵入検知と同様、侵入を検知した後の対策として、アラート配信、警告、アクセス遮断、感染データ削除等に言及する事項として定義する。

ログ解析、リバースエンジニアリングは、更にログ解析とリバースエンジニアリングに分類できる。このうち、ログ解析は、システム内に収集、蓄積されるログを解析する技術として定義する。ログ解析には、監視インシデントや、解析対象ログ、解析内容、ログの収集方法、管理方法、解析手法、アクションが含まれる。他方、リバースエンジニアリングは、ソフトウェアの解析技術であり、プログラム（ソースコードのないバイナリコード）に対して逆アセンブル、逆コンパイルを実施し、第三者が解読できるコードに変換して、バイナリコードの動作を解析する技術として定義する。リバースエンジニアリングには、解析対象、解析手法、アクションが含まれる。

暗号技術は、データの内容を第三者が判別できないようにするための技術であり、データそのものを何らかの方法で符号化し、容易には解析・解読できないような形式に変換、保存、通信するための技術の総体として定義する。暗号技術には、暗号プリミティブ、暗号利用基礎プロトコル、暗号利用応用プロトコル、対実装攻撃対策、安全性評価手法、暗号危殆化対策が含まれる

認証技術は、ネットワーク上のエンティティを特定するための電子認証技術に関し、個人認証、回線認証、クライアント・サーバ認証、認証連携の４つの認証に関する事項の総体として定義する。個人認証、回線認証、クライアント・サーバ認証の３つの認証技術には、トークン、クレデンシャル管理、認証プロセス、アサーション（認可）等が含まれる。

２．調査対象課題

本調査では、調査対象の課題を、「脅威・攻撃等の早期発見・早期対処」、「脅威・攻撃等に対する防御能力の向上」、「効率的なセキュリティ運用の推進」の３つの課題分類で整理する。

このうち、脅威・攻撃等の早期発見・早期対処は、入口での初期潜入の監視・診断・分析精度の向上、潜入後の IT システムでの基盤構築（不審な動き）の監視・診断・分析精度の向上、潜入後の内部侵入の監視・診断・分析精度の向上の３つに言及する事項に加え、さらに近年注目されるものとして、未知の攻撃の監視・診断・分析精度の向上等に言及する事項も含めて定義する。

脅威・攻撃等に対する防御能力の向上は、IT システムそのもののセキュリティ向上と IT システムが扱う情報のセキュリティ向上等に言及する事項として定義する。

効率的なセキュリティ運用の推進は、低コスト化対応や自動化、人手による運用の負荷軽減、処理速度の向上、運用環境の改善、セキュリティ人材の育成（教育・訓練・演習）等に言及する事項として定義する。

３．調査対象適用領域・用途

本調査では、調査対象の適用領域・用途を、「国家安全保障に関わる情報システム」、「企業等の情報システム（PC、サーバ等）」、「制御系システム、組込みソフト」、「IT サービス、IT 機器」の４つの適用領域・用途で整理する。

このうち、企業等の情報システム（PC、サーバ等）は、個人情報・営業秘密情報の保護、コンテンツの保護(ファイル送付、文書管理等)、DRM(Digital Rights Management)、著作権の保護、決済・課金の保護、内部統制、ガバナンス、証憑の管理、国内外の拠点管理、提供サービス、オンライン手続の保護、リスク管理、コンプライアンス等に言及する事項として定義する。

制御系システム、組込みソフトは、重要インフラの保護、住宅、情報家電の保護、自動車の保護、医療機器の保護、航空宇宙関係の保護、ファクトリーオートメーションの保護等に言及する事項として定義する。

IT サービス、IT 機器は、セキュアなデバイス（PC、サーバ等）、セキュアな入退管理システム、セキュアなクラウドコンピューティング、セキュアな通信、セキュアなサービスプラットフォーム、セキュアなアプリケーション、セキュアなリモートアクセス（テレビ会議、在宅勤務等）等言及する事項として定義する。

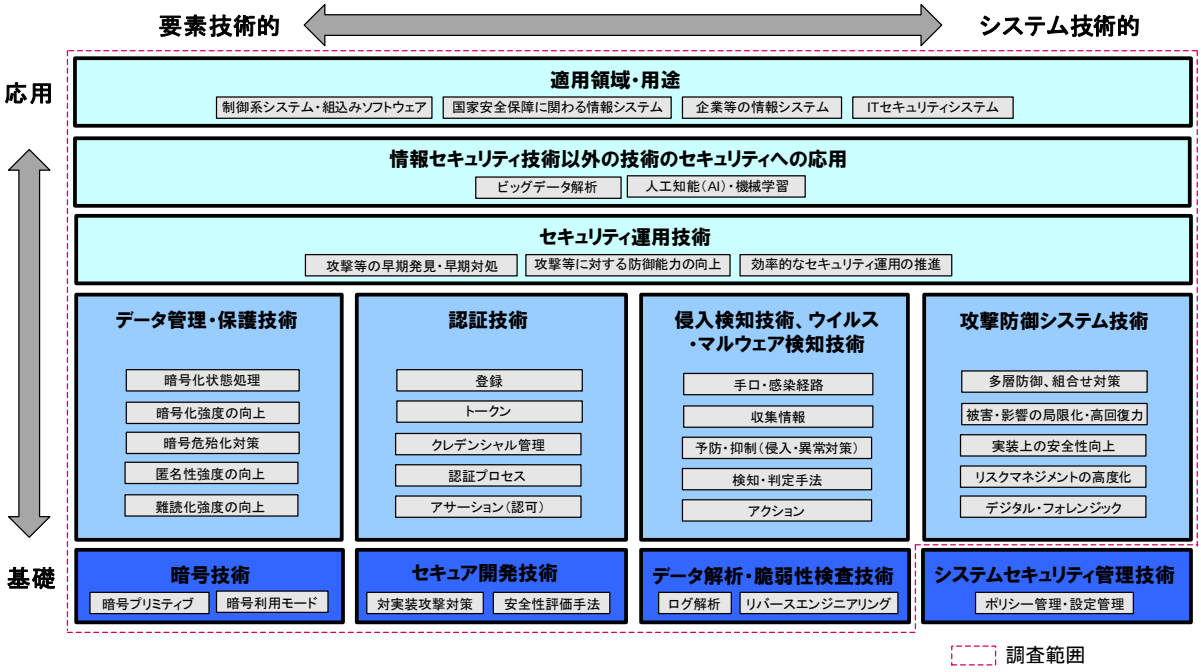
４．調査対象技術範囲

本調査では、「侵入検知、ウイルス・マルウェア検知」、「ログ解析、リバースエンジニアリング」、「暗号技術」、「認証技術」の４つの調査対象技術と、調査対象課題、調査対象適用領域・用途を組み合わせた範囲が、調査対象技術範囲である。

調査対象技術範囲を示した図が以下の図である。なお、情報セキュリティ技術分野は広くかつ複雑であり、体系的かつ俯瞰的に整理された図は見当たらない。そのため、

国立研究開発法人科学技術振興機構　研究開発戦略センターが取りまとめた「研究開発の俯瞰報告書　情報科学技術分野（2015 年）」に記載されているセキュリティーの俯瞰図を参考にして、縦軸に基礎か応用かを、横軸に要素技術的かシステム技術的かを取り、本調査対象技術を位置付けると、以下の図のように整理することができる。

図 2-1
情報セキュリティ技術の概念



なお、セキュリティポリシーの管理や設定管理に関わる技術は、情報セキュリティ技術には含めないものとした。

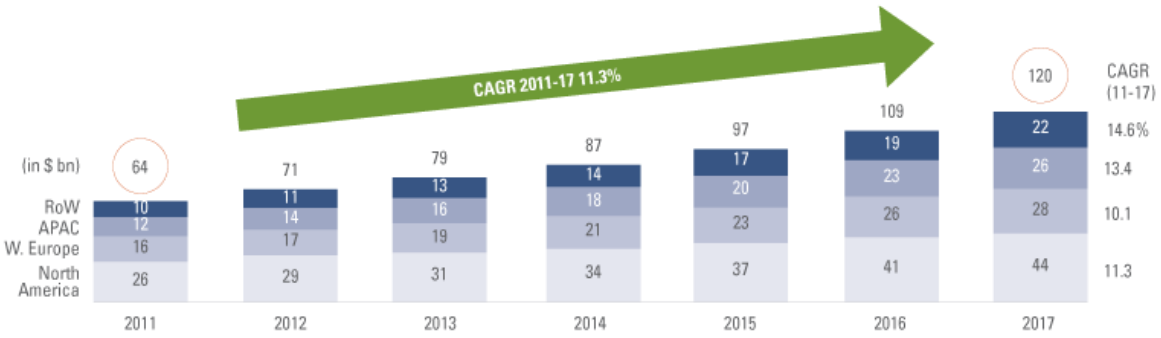
第３章　市場環境調査・分析

第１節　情報セキュリティ技術分野のグローバル市場動向

グローバルにおける情報セキュリティ技術分野の市場は、2011 年の 640 億 US ドルから、年次成長率 11.3%で成長を続け、2017 年には 1,200 億 US ドルまで成長すると見られている。

地域別の内訳をみると、2011 年では北米地域が約 41%を占めている。一方、2017 年時点では、北米地域の割合は約 37%程度となり、代わって西欧、アジア太平洋、その他地域の割合が相対的に高まると見られている。

図 3-1
情報セキュリティ技術分野のグローバル市場動向



APAC：Asia Pacific, **CAGR**：Compound Annual Growth Rate, **RoW**：Rest of World, **W.Europe**：Western Europe

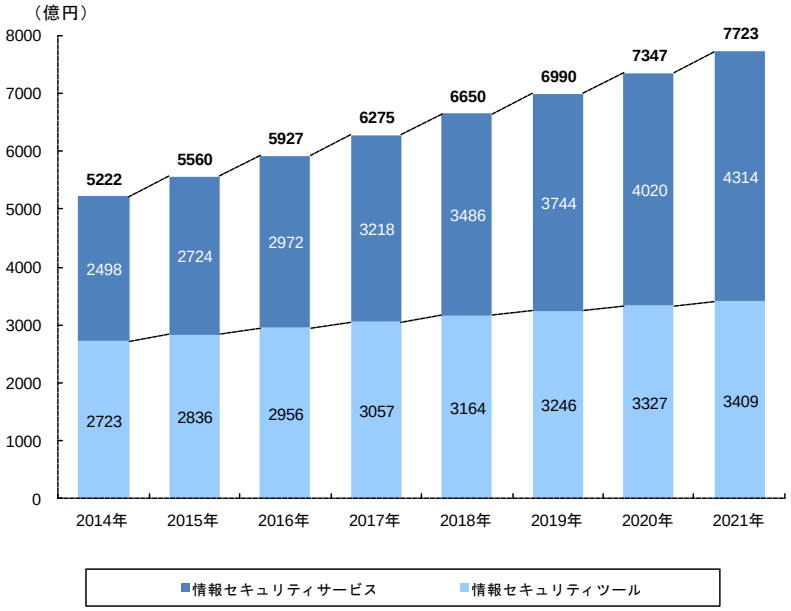
Sources：MarketsandMarkets；Global Industry Analysts 2012；AlixPartners analysis

出所）AlixPartners Web site

第２節　情報セキュリティ技術分野の日本市場動向

日本の法人向け情報セキュリティ市場は、2014 年に約 5,200 億円であったが、その後、市場規模を大きく伸長し、2021 年には 7,700 億円を超える規模に達するものと予測されている。

図 3-2
日本の法人向け情報セキュリティ市場規模予測



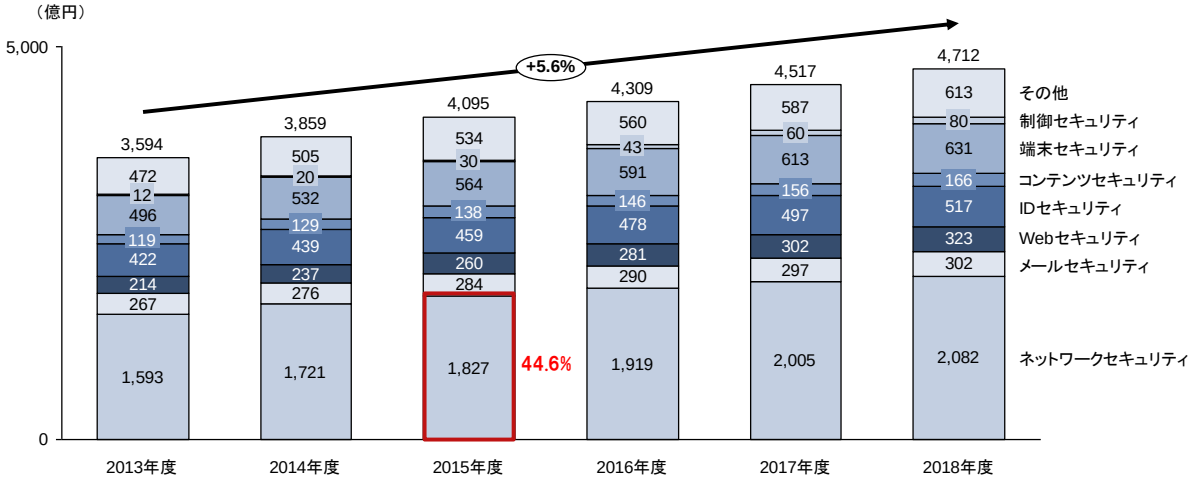
出所）野村総合研究所「IT ナビゲーター2016 年度版」

別のデータで見ると、日本国内における情報セキュリティ技術分野の市場は、2015 年時点で約 4,095 億円程度であり、2013 年度から 2018 年度にかけて、年次成長率 5.6%で市場

規模が拡大している。

市場の内訳についてみると、最も割合が高いのはネットワークセキュリティ関連で、2015年度時点で約1,827億円、割合にして市場全体の約44.6%を占める。その他では、端末セキュリティ、IDセキュリティなどの割合が比較的高い。

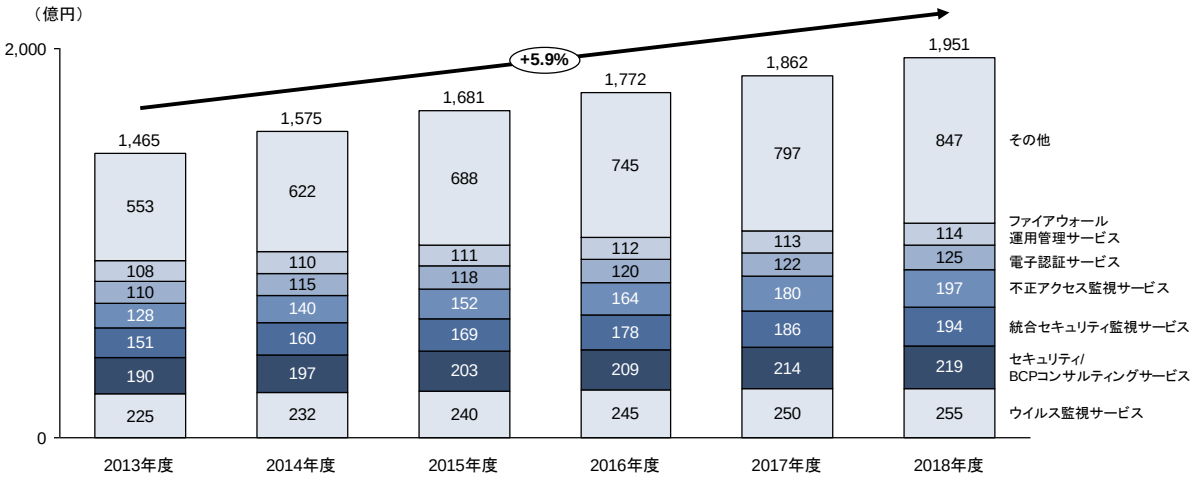
図 3-3
情報セキュリティ技術分野の日本市場動向



出所）富士キメラ総研「2014 ネットワークセキュリティビジネス調査総覧」より野村総合研究所作成
注）2013 年度は実績、2014 年度は見込み、2015 年度以降は予測値

国内市場をサービス/製品別に分類してみると、国内のセキュリティサービス市場は、2013年度から2018年度にかけて、年次成長率5.9%で拡大している。商材別にみると、2015年時点で、市場規模が最も大きいのは、ウイルス監視サービスで約240億円である。その他では、セキュリティ/BCPコンサルティングサービス、統合セキュリティ監視サービス、不正アクセス監視サービス、電子認証サービス、ファイアウォール運用管理サービスの市場規模が比較的大きい。

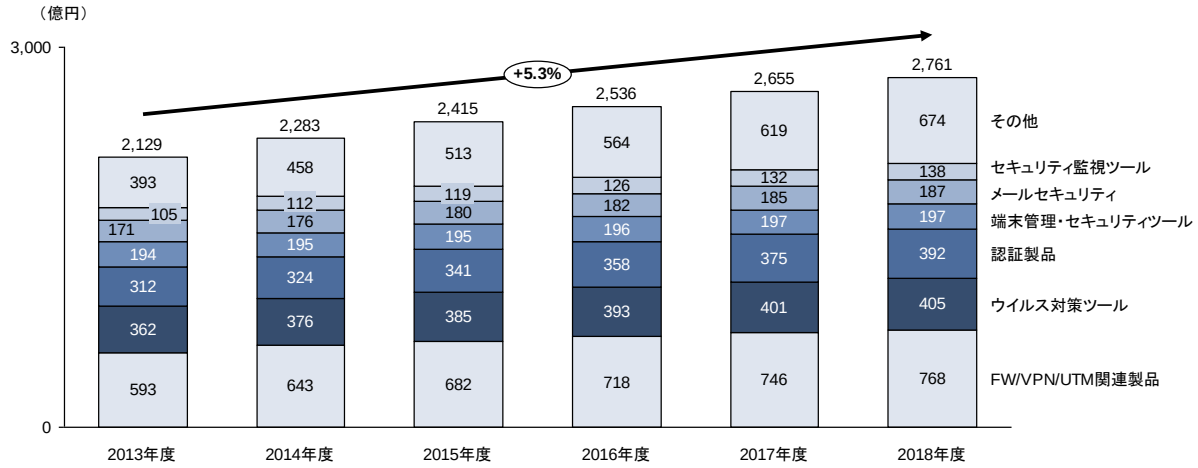
図 3-4
日本のセキュリティサービス市場（商材別）



出所）富士キメラ総研「2014 ネットワークセキュリティビジネス調査総覧」より野村総合研究所作成
注）2013 年度は実績、2014 年度は見込み、2015 年度以降は予測値

他方、国内のセキュリティ製品市場は、2013 年度から 2018 年度にかけて、年次成長率 5.3%で拡大している。商材別にみると、2015 年時点で、市場規模が最も大きいのは、ファイアウォール/VPN/UTM 関連製品で約 682 億円である。その他では、ウイルス対策ツール、認証製品、端末管理・セキュリティツール、メールセキュリティ、セキュリティ監視ツールの市場規模が比較的大きい。

図 3-5
日本のセキュリティ製品市場（商材別）



出所）富士キメラ総研「2014 ネットワークセキュリティビジネス調査総覧」より野村総合研究所作成
注）2013 年度は実績、2014 年度は見込み、2015 年度以降は予測値

第４章　政策動向調査・分析

各国のサイバーセキュリティに関する政策について、①研究開発における重点分野、②研究開発の推進体制、③サイバーセキュリティ産業の振興といった３つの視点から概観したものが以下の表である。

表 4-1
各国のサイバーセキュリティに関する政策の概観

論点	日	米	EU	韓	中	イスラエル
研究開発における重点分野	2014 年に改訂された NISC の開発計画、および先述の SIP において、重要インフラ保護、IoT、モバイル、クラウド等が掲げられる。	CSIA の研究開発計画（Trustworthy Cyberspace）によれば、クラウドやモバイル、IoT、重要インフラ分野の研究開発	HORIZO2020 については、本年度から募集が開始されたばかりであり、まだ募集分野が限られている。	応用分野ではモバイル環境やクラウド、IoT/M2M、ビッグデータ等の開発を行っている。	政府研究機関の研究開発計画については、あまり公開されていない。	重点分野についてはあまり情報が公開されていない。
研究開発の推進体制	内閣府戦略的イノベーション創出プログラム（SIP)に重要インフラサイバーセキュリティが設置されたが、期限つき。他方 NISC は常設であるが、総合調整が主で予算配分権限なし。	NITRD、特にサイバーセキュリティに特化した CSIA が中心的な役割を担って研究開発の調整を行っている。なお、予算要求は各省庁ではなく、CSIA として行われている。	研究開発は競争資金配分計画である HORIZON 2020 を通じて実施されており、同計画は欧州委員会の科学技術部門（JRC）が所管している。	サイバーセキュリティの研究開発に関しては、日本の総務省および経済産業省、文部科学省等に当たる省庁を統合した未来創造部が実施しており、実質的に一元化されている。	国家発展委員会の中にサイバーセキュリティに関する委員会を設置。	日本同様、基本的には各官庁に設置されたチーフサイエンティストが研究開発予算を配分する。ただし、これらサイエンティストは基本的に民間または学会の研究者である。
サイバーセキュリティ産業の振興	2014 年に改訂された NISC の研究開発計画、および SIP においても研究開発成果の早期のビジネス化が規定されているが、具体的な施策は未定である。	Trustworthy Cyberspace で、早期の事業化を規定。官民共同研究施設の設置や政府保有特許のカタログ化等を実施。政府機関の研究者が起業した企業を積極的に政府機関が活用して産業を振興。	研究開発の基本計画である HORIZO2020 は商用化を前提とした研究開発プログラムである。また、域内市場の統合（セキュリティ関連規格の統一など）によって産業振興を実施しようとしている。	ETRI 等の研究機関が民間への技術移転を前提とした研究開発を行っている。また、政府機関の研究者が起業した企業を積極的に政府機関が活用することで産業を振興している。	政府や重要インフラ企業に監査義務を導入することで国産品の調達を進める。また金融分野では IT 投資の一定額をセキュリティに振り分けさせるなどして、セキュリティ産業振興を行う。	各省のチーフサイエンティストが成果のビジネス化を所管する。国家サイバー局が独自のファンドで産業育成を行う。政府機関の研究者が起業した企業を積極的に政府機関が活用して産業を振興。

第１節　研究開発における重点分野

研究開発の重点分野に関しては、情報が十分収集できなかった中国・イスラエルを除いては、おおむね同様の傾向を示しているといえる。すなわち、各国とも、通信・交通等の重要インフラ保護、IoT、モバイル、クラウドへの対応等を掲げているのである。

これは、IoT の進展やスマートフォンの普及とそれに伴うモバイル環境でのサイバー攻撃の脅威の増大、クラウドサービスの進展等、サイバーセキュリティが必要となる背景が共通しているためと考えられる。

重点分野には先進国で共通のニーズがあるということができ、これは一義的には我が国サイバーセキュリティ企業の国際展開にとって追い風であるが、逆にいえば海外から日本市場に容易にセキュリティ製品が流入する恐れがあることも示している。

第２節　研究開発の推進体制

研究開発の推進体制については、特に米・EU・韓と日本の間で大きな差異がある。すなわち、米国や EU、韓国では総合調整に加え予算配分権限をも持ったサイバーセキュリティの研究開発における司令塔的な組織が存在している。たとえば、米国では 20 年以上を数える NITRD、とりわけその中の CSIA が研究開発に関する総合調整、予算の請求・配分を通じて司令塔的な役割を担っている。対して、日本にはサイバーセキュリティに特化した、常設の予算配分権限を持った司令塔が存在していない。

第３節　サイバーセキュリティ産業の振興

米国のほか、ヒアリングによればイスラエルや韓国でも、政府機関から独立したサイバーセキュリティに関する起業者を、元の所属先等の政府機関が積極的に使用する流れがあり、それが国産サイバーセキュリティ製品・企業の新興につながっている。

また、中国では投資額のうち一定額をサイバーセキュリティへの投資に振り向けさせるなど、国家が規制によって国産セキュリティ製品を優遇することで、国内産業を育成している。

他方、日本では政府・民間を問わずこのような国産製品や日本企業を積極的に支援しようという意識が希薄であり、たとえば政府が技術開発に対する補助金等の支援を行っても、それ以降の調達やマーケティングに対する支援は行われていない。

第４章　特許動向調査・分析

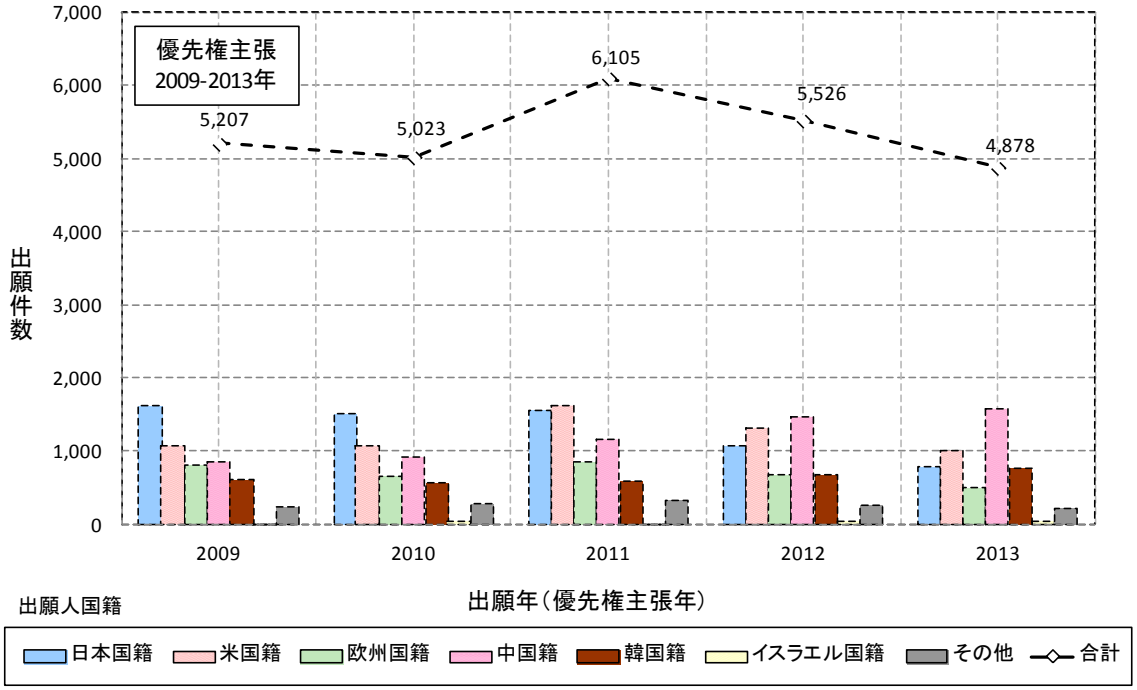
第１節　全体動向調査・分析

出願人国籍別出願件数推移を以下の図に示す。調査対象期間内における特許出願件数は、およそ 26,739 件である。これを推移でみると、2009 年から 2010 年にかけて微減傾向であ

ったが、2011 年に増加に転じ、2009 年を上回る水準にまで件数を大きく伸ばしている。

また、出願人国籍別の出願件数推移についてみると、日本国籍の出願人による出願件数は、欧州国籍の出願人による出願件数や韓国籍の出願人による出願件数と共に、ほぼ横ばいの状態である。他方、米国籍、中国籍の出願人による出願件数は増加傾向が見られる。2011 年時点で日本国籍の出願人による出願件数は、米国籍の出願人による出願件数に追い抜かれ、首位の座を明け渡している。

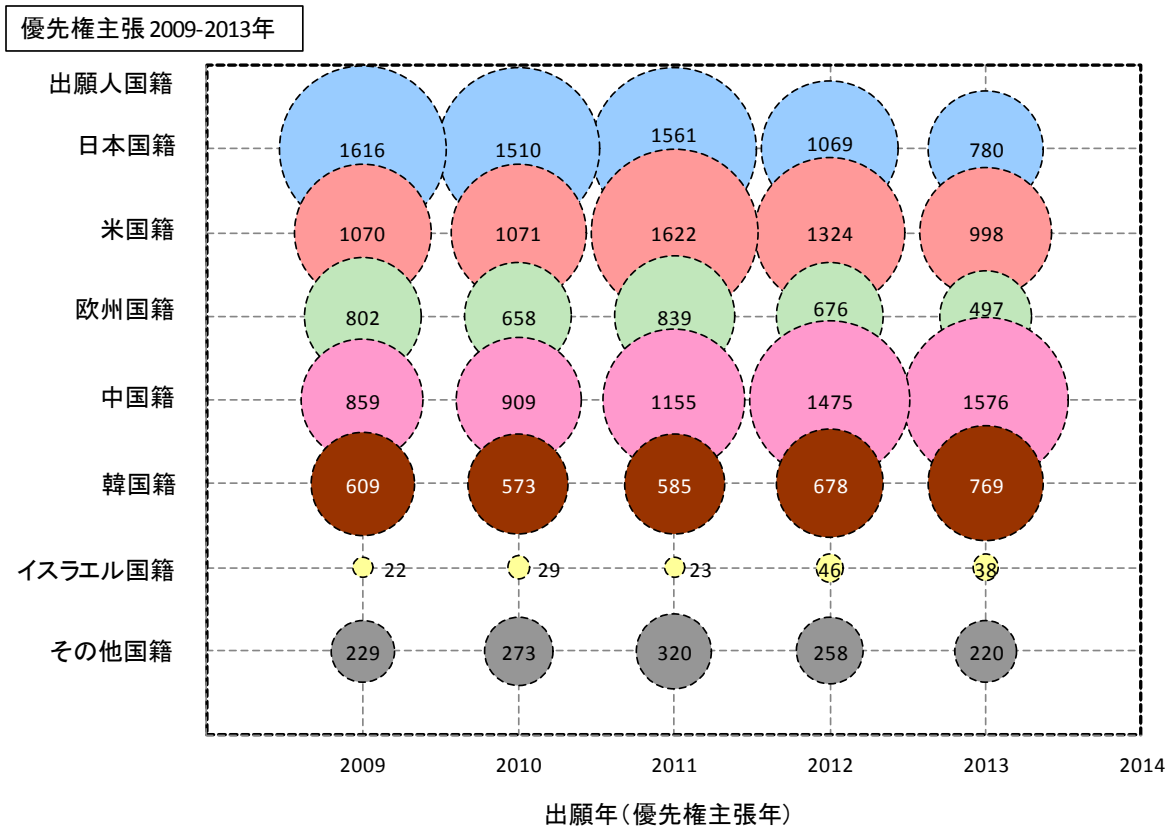
図 4-1
出願人国籍別出願件数推移



注）2012年以降は、データベース収録の遅れ、PCT出願の各国移行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。

出願人国籍別登録件数推移を以下の図に示す。調査対象期間内における特許登録件数は、およそ 8,519 件であり、特許出願件数 26,739 件の 3 割以上を占める。また、出願人国籍別の登録件数推移についてみると、日本国籍の出願人による登録件数は、2009 年から 2011 年までの 3 年間において、概ね横ばいの状態である。韓国籍の出願人による登録件数についても、日本国籍の出願人と同様、概ね横ばいの状態である。他方、米国籍や欧州国籍、中国籍の出願人による登録件数は共に 2010 年から 2011 年にかけて、大幅な増加傾向が見られる。

図 4-2
出願人国籍別登録件数推移



注）調査時点で審査請求前や審査中の出願が存在するため、2013年に近づくにつれて件数が減少することに注意すること。

出願先国別－出願人国籍別出願収支、出願先国別－出願人国籍別登録収支のいずれにおいても、自国への出願、自国での登録が圧倒的に多く、日本国籍の出願人が、米国を除き、欧中韓イスラエルでのビジネスをそれほど重視していない状況が見受けられる。このような状況となっている背景には、国内市場の安定性や海外市場の開拓の難しさが影響しているものと考えられる。

図 4-3

出願先国別－出願人国籍別出願件数収支

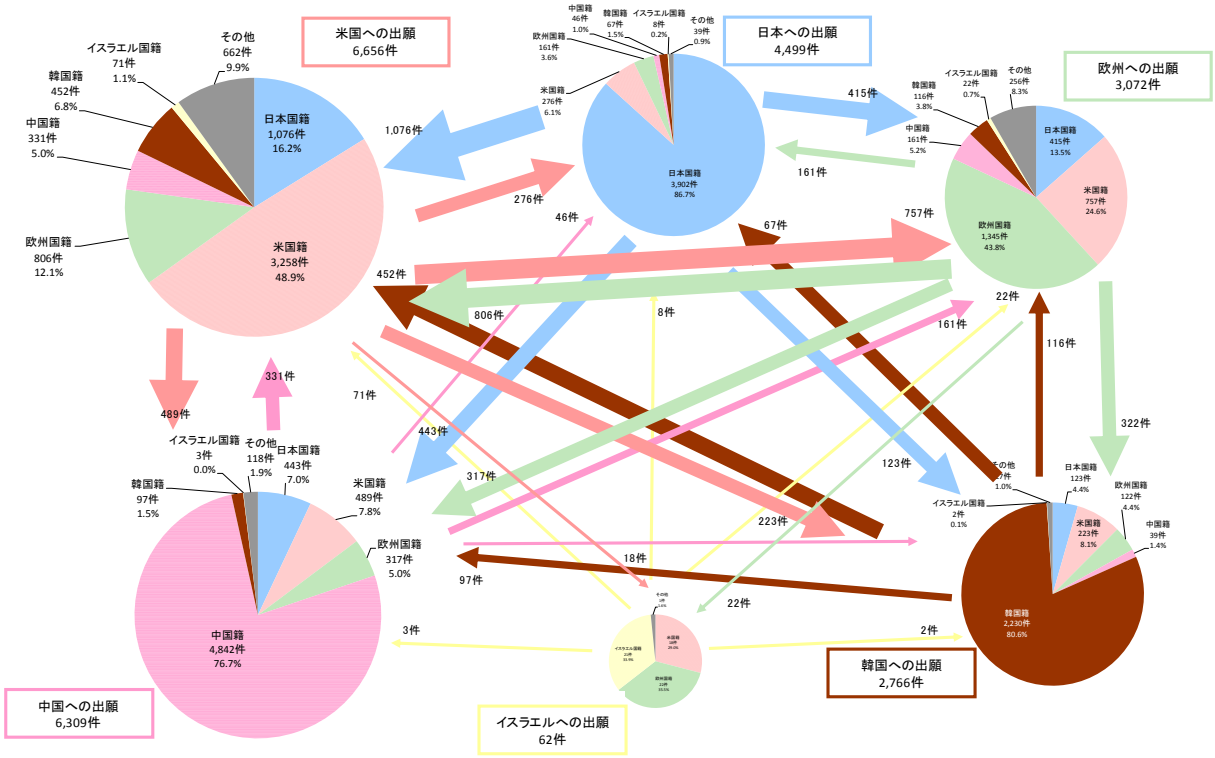
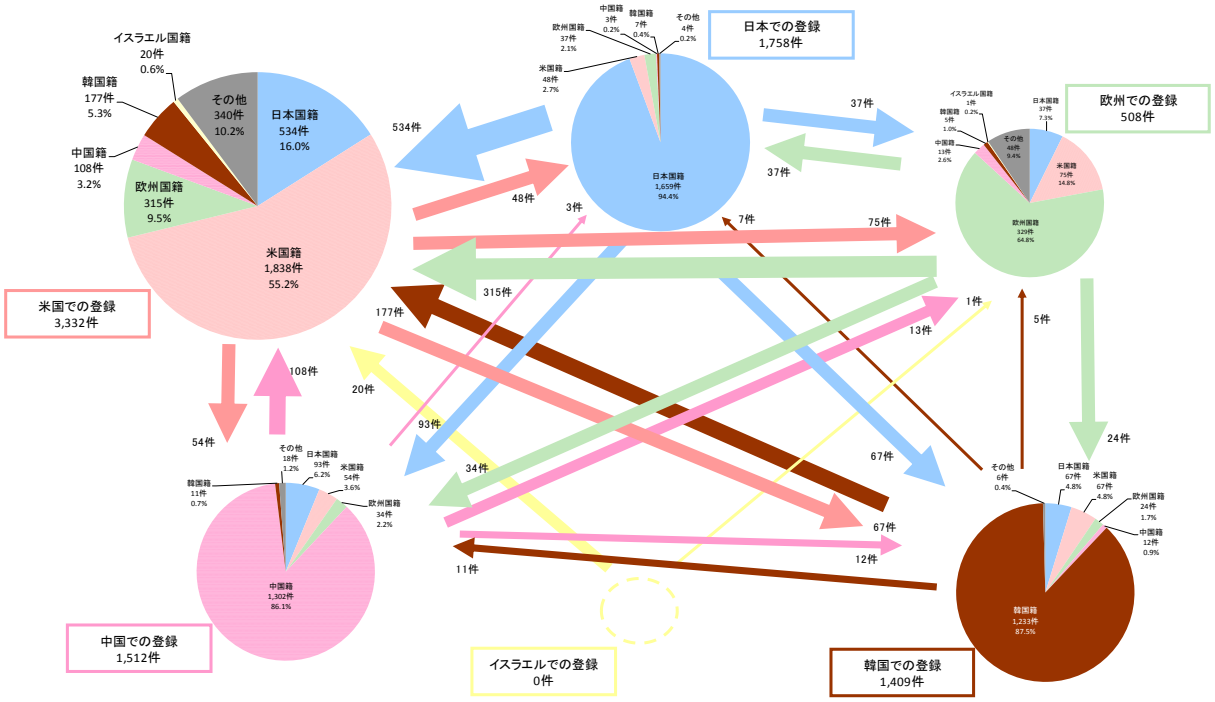


図 4-4

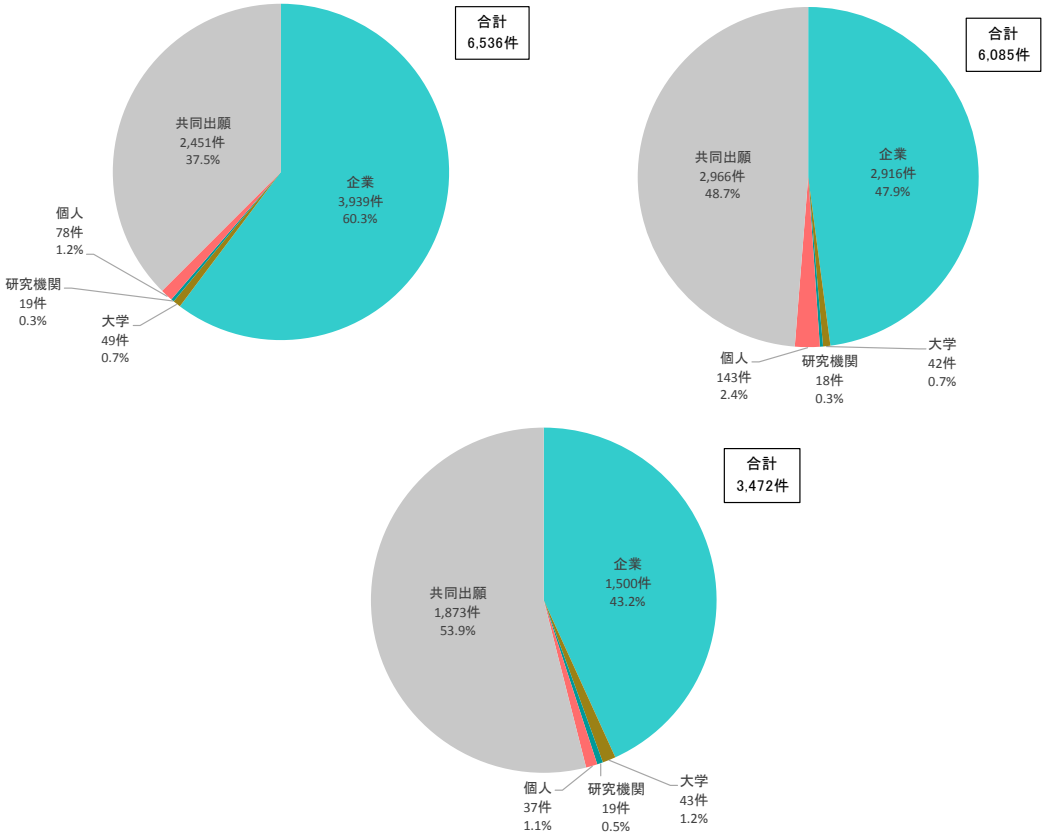
出願先国別－出願人国籍別登録件数収支



次に、出願人国籍別－出願人属性別出願件数比率についてみると、日本国籍の出願人に関しては、企業からの出願件数が 3,939 件と最も多く、全体の 60.3%を占める。

他方、米国籍の出願人に関しては、共同出願の出願件数が 2,966 件と最も多く、全体の 48.7%を占める。また、欧州国籍の出願人に関しても、共同出願の出願件数が 1,873 件と最も多く、全体の 53.9%を占める。米国籍の出願人、欧州国籍の出願人と日本国籍の出願人を比較すると、共同出願の出願件数の割合に大きな開きが見られる。

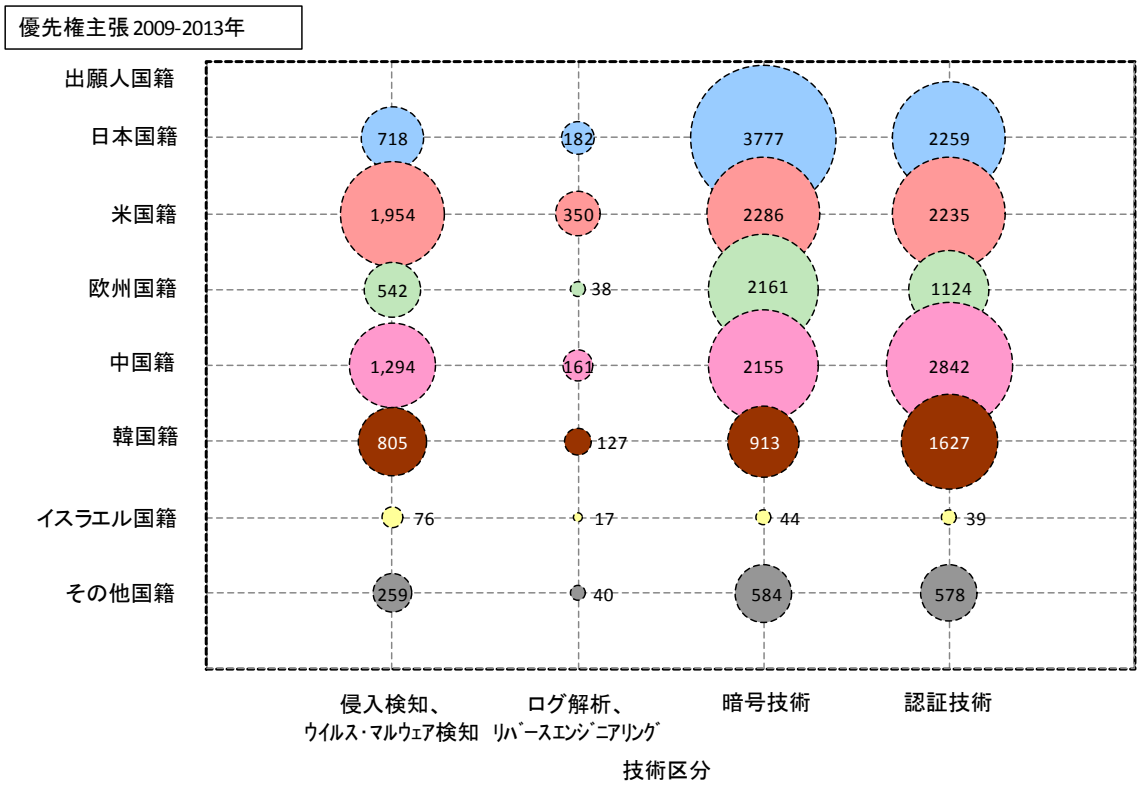
図 4-5
出願人国籍別－出願人属性別出願件数比率
（上左図は日本国籍の出願人、上右図は米国籍の出願人、下図は欧州国籍の出願人）



第２節　技術区分別動向調査・分析

技術区分別－出願人国籍別出願件数を見る限り、情報セキュリティ技術分野における日本国籍の出願人による特許出願の特徴として、暗号技術や認証技術に関わる特許出願への偏重傾向が浮き彫りになっている。巧妙化・複雑化する攻撃手法に対する継続的な対策技術開発の必要性を考慮すると、侵入検知、ウイルス・マルウェア検知やログ解析、リバースエンジニアリングといった情報セキュリティ技術についても、暗号技術や認証技術とほとんど遜色がないレベルで特許出願が可能となるよう技術開発の強化をより一層強力に推進していく必要がある。

図 4-6
技術区分別－出願人国籍別出願件数



第３節　出願人別動向調査・分析

出願人別出願件数上位ランキングを下の表に示す。情報セキュリティ技術に関わる出願件数全体でみると、多くの日本の IT ベンダー、通信キャリアがランキングの 10 位以内にランクインしているが、圧倒的に優勢と呼べるほどではない。

日本の IT ベンダーでは、東芝が 551 件、富士通が 520 件、ソニーが 481 件、日本電気が 448 件、日立製作所が 339 件と 10 位以内であり、20 位以内である三菱電機（327 件）、パナソニック（262 件）、キヤノン（230 件）を含めると、概ねすべての大手 IT ベンダーが上位に顔を並べる。また、IT ベンダー以外では、通信キャリアである日本電信電話が 10 位以内にランクインしている。

また、海外の IT ベンダーでは、米国の IBM（542 件）、韓国の SAMSUNG（521 件）、米国の INTEL（495 件）、中国の ZTE（428 件）が 10 位以内にランクインしている。

表 4-2
出願人別出願件数上位ランキング（全体）

順位	出願人名	出願件数
1	TOSHIBA	551
2	IBM（米国）	542
3	SAMSUNG（韓国）	521
4	FUJITSU	520
5	INTEL（米国）	495
6	SONY	481
7	NEC	448
8	NTT	434
9	ZTE（中国）	428
10	HITACHI	339
11	TENCENT TECHNOLOGY SHENZHEN（中国）	328
12	MITSUBISHI ELECTRIC	327
13	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE（韓国）	307
14	QUALCOMM（米国）	292
15	HUAWEI TECHNOLOGIES（中国）	286
16	MICROSOFT（米国）	272
17	PANASONIC	262
18	CANON	230
19	MCAFEE（米国）	212
20	SIEMENS（欧州）	206

ウイルス・マルウェア検知やリバースエンジニアリングに関する出願人別出願件数上位ランキングについてみると、日本国籍の出願人は、10 位以内に 1 社もランクインしていない状況である。

表 4-3
ウイルス・マルウェア検知に関する出願人別出願件数上位ランキング

順位	出願人名	出願件数
1	TENCENT TECHNOLOGY SHENZHEN（中国）	180
2	MCAFEE（米国）	167
3	BEIJING QIHOO SCI & TECHNOLOGY（中国）	152
4	IBM（米国）	139
5	SYMANTEC（米国）	116
6	SAMSUNG（韓国）	112
7	INTEL（米国）	102
8	AHNLAB（韓国）	97
9	F SECURE（欧州）	91
10	KASPERSKY LAB STOCK（ロシア）	89
11	MICROSOFT（米国）	77
12	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE（韓国）	44
13	QUALCOMM（米国）	43
14	HEWLETT-PACKARD DEV（米国）	40
15	CISCO TECHNOLOGY（米国）	31
16	GOOGLE（米国）	30
17	HITACHI	27
18	RAYTHEON （米国）	25
18	BEIJING JINSHAN NETWORK TECHNOLOGY（中国）	25
20	ZTE（中国）	24
20	HUAWEI TECHNOLOGIES（中国）	24

表 4-4
リバースエンジニアリングに関する出願人別出願件数上位ランキング

順位	出願人名	出願件数
1	IBM（米国）	66
2	TENCENT TECHNOLOGY SHENZHEN（中国）	39
3	KASPERSKY LAB STOCK（ロシア）	20
4	BEIJING QIHOO SCI & TECHNOLOGY（中国）	15
5	VERISIGN（米国）	14
5	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE（韓国）	14
7	RAYTHEON （米国）	13
7	AHNLAB（韓国）	13
9	MCAFEE（米国）	12
9	HEWLETT-PACKARD DEV（米国）	12
11	MITSUBISHI ELECTRIC	11
11	SYMANTEC（米国）	11
11	HITACHI	11
11	KOREA INTERNET & SECURITY AGENCY（韓国）	11
15	NTT	8
15	KDDI	8
17	PALO ALTO NETWORKS（米国）	7
17	BEIJING JINSHAN NETWORK TECHNOLOGY（中国）	7
19	LOOKOUT（米国）	6
20	BEIJING ANTIY ELECTRONIC APPLIANCE（中国）	5
20	FUJITSU	5
20	FFRI	5
20	JAPAN SCI & TECHNOLOGY AGENCY	5
20	MICROSOFT TECHNOLOGY LICENSING （米国）	5
20	INTEL（米国）	5

他方、ログ解析の分野で出願人別出願件数上位ランキングの上位にランキングされている UBIC や、リバースエンジニアリングの分野で出願人別出願件数上位ランキング 20 位以内にランキングされている FFRI のように、日本のベンチャー企業が台頭する動きも見られる。

このようなベンチャー企業の技術開発、研究開発の取組みが活性化するよう政府機関等が後押ししつつ、侵入検知、ウイルス・マルウェア検知、ログ解析、リバースエンジニアリングといった技術分野においても、暗号技術や認証技術と同様、競争優位性を確立できるようにすることが必要である。

表 4-5
ログ解析に関する出願人別出願件数上位ランキング

順位	出願人名	出願件数
1	UBIC	30
2	HEWLETT-PACKARD DEV(米国)	18
3	MITSUBISHI ELECTRIC	15
4	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE(韓国)	13
5	NTT	10
6	INTEL(米国)	9
7	BOEING(米国)	8
8	SYMANTEC(米国)	7
8	F SECURE(欧州)	7
10	INCA INTERNET(韓国)	6
10	ALIBABA GROUP HOLDING(ケイマン諸島)	6
12	EVIDENCE TALKS(欧州)	5
12	KOREA INTERNET & SECURITY AGENCY(韓国)	5
14	OPTIM	4
14	JUNIPER NETWORKS(米国)	4
14	FORTINET(米国)	4
14	FUJITSU	4
14	FRONS(韓国)	4
14	GENERAL ELECTRIC(米国)	4
14	TOKAI RIKA DENKI	4
14	GIESECKE & DEVRIENT(欧州)	4
14	DAINI DENDEN	4
14	UNIV NORTH CAROLINA(米国)	4
20	WINS TECHNET(韓国)	4
20	FUJI FILM	3
20	NANO SAFETY(ロシア)	3
20	OBERTHUR TECHNOLOGIES(欧州)	3
20	BEIJING QIHOO SCI & TECHNOLOGY(中国)	3
20	KASPERSKY LAB STOCK(ロシア)	3
20	NEC	3

第４節　注目出願人の調査・分析

出願件数の増加傾向が見られる米国籍、中国籍の出願人のうち、その中でも出願件数が上位にランキングされている IBM（米国）、INTEL（米国）、ZTE（中国）、TENCENT TECHNOLOGY SHENZHEN（中国）の技術区分別の出願件数推移についてみると、IBM（米国）では、侵入検知やウイルス・マルウェア検知の予防・抑制（侵入・異常対策）といった技術分野や、IT システムが扱う情報のセキュリティ向上のための検知精度の向上、漏えい危険性の低下、不正利用防止といった課題分野の出願件数が件数を大幅に伸ばしている。また、INTEL（米国）では、ブロック暗号やハッシュ関数、暗号利用基礎プロトコルとしての守秘・秘匿、鍵管理、鍵生成といった暗号技術分野や、IT システムが扱う情報のセキュリティ向上のための漏えい危険性の低下、不正利用防止、認証精度・安全性向上といった課題分野、セキュアなデバイスやセキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。主要な米国企業における技術開発競争としては、巧妙化・複雑化する攻撃手法への対策やそれらの攻撃から情報を守るための対策が中心となっている。

他方、ZTE（中国）では、鍵生成や SIM カードといった技術分野や、IT システムが扱う情報のセキュリティ向上のための漏えい危険性の低下、認証精度・安全性向上といった課

題分野、セキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。また、TENCENT TECHNOLOGY SHENZHEN（中国）では、ウイルス・マルウェア検知の予防・抑制（侵入・異常対策）としてのウイルス対策や検知・判定手法としてのパターンマッチング手法、回復アクション、顔認証といった技術分野や、ITシステムが扱う情報のセキュリティ向上のための検知精度の向上、認証精度・安全性向上といった課題分野、セキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。主要な中国企業における技術開発競争としては、ウイルス・マルウェアへの対策やそれらの攻撃から情報を守るための対策、生体認証、モバイルコンピューティング分野のセキュリティ向上が中心となっている。

第５節　注目特許の調査・分析

訴訟係属特許情報や審判情報、ITC（米国国際貿易委員会）に係属した特許情報、被引用特許数ランキング上位特許情報、被引用数ランキング上位非特許文献情報をもとに注目特許を分析すると、サンドボックスやパスワードのセキュリティシステムに関わる特許のほか、ウイルス・マルウェア検知や侵入検知、認証技術に関わる幾つかの特許が注目特許として抽出された。なかでも特に、ウイルス・マルウェア検知分野の注目特許が多く挙がっており、当該分野が現在の市場競争の主戦場になっていることを裏付ける結果となっている。当該分野で既に海外のプレイヤーが優位なポジションを築いている中で、今後、日本のプレイヤーが存在感を高めていくためには、新技術・製品分野の技術開発や製品化において活路を見出していくことが重要になっている。

表 4-6
被引用特許数が多い特許の上位ランキング

	被引用特許数	特許番号	タイトル	出願人
①	93	US20110078081	モバイル支払アプリケーション･アーキテクチュア	VISA INT SERVICE ASSOC
②	68	US20120278886	マルウェアの検出およびフィルタリング	SEVEN NETWORKS INC
③	68	US20120079596	マルウェアの自動検出および分析のための方法およびシステム	VERISIGN INC
④	67	US8375225	メモリ保護	WESTERN DIGITAL TECHNOLOGIES INC
⑤	61	US20120280783	携帯用電子機器を使用してロック機構を制御するためのシステム	APIGY INC
⑥	57	US20120222120	マルウェア検出方法および移動端末	SAMSUNG ELECTRONICS CO LTD
⑦	56	US20110041179	マルウェア検出	F SECURE CORP
⑧	55	US20100269008	分散データストレージシステムデータの復号化および暗号解読	CLEVERSAFE INC
⑨	54	US20120280790	携帯用電子機器を使用してロック機構を制御するためのシステム	APIGY INC
⑩	53	US20130031600	モバイルデバイス上で悪意のあるトラフィックのためのモバイルアプリケーション動作の監視	SEVEN NETWORKS INC
⑪	53	US20110270751	電子商取引システムのシステムおよび方法	BRADLEY J ほか
⑫	53	JP2010268417	記録装置及びコンテンツデータ再生システム	TOSHIBA KK
⑬	50	US8613070	シングルサインオンアクセス	CITRIX SYSTEMS INC

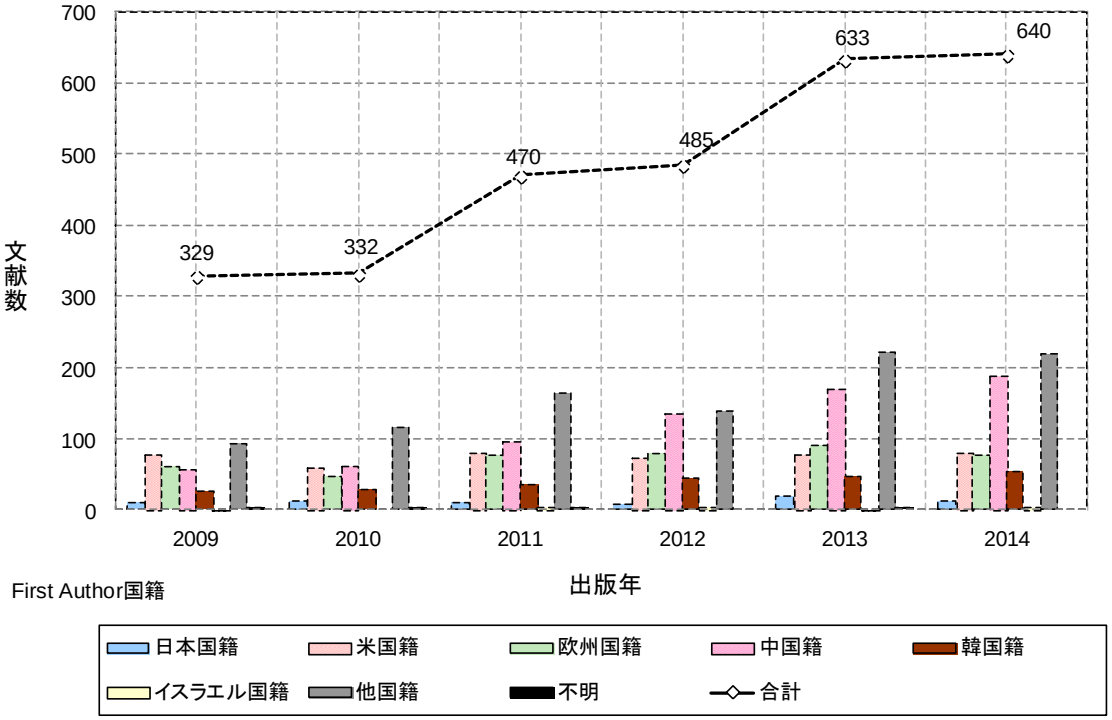
第５章　研究開発動向調査

第１節　全体動向調査・分析

Web of Science における、2009 年から 2014 年にわたる研究者所属機関国籍別論文発表件数の推移を以下に示す。日本、米国、欧州、中国、韓国、イスラエル、その他の国々を合計した値は、大きく増加傾向にある。2009 年段階では 329 本の論文数であったものが、2014 年では 640 本に達している。

各国の中で、特に発表件数の増加が著しいのが中国である。

図 5-1
研究者所属機関国籍別論文発表件数推移（Web of Science）



なお、本分析で用いた論文が掲載されている、掲載誌の発行主体/学会のランキングを以下の図に示す。日本の研究者が多くは投稿することのない Springer 等が上位にきていることからも分かる通り、Web of Science に収録されている論文に一定の偏りが存在していることから、本分析は必ずしも世界的な実情を客観的に示しているのではなく、あくまで Web of Science に収録されている論文に関して分析したことを明示しておくこととする。

図 5-2
研究者所属機関国籍別論文発表件数比率（Web of Science）

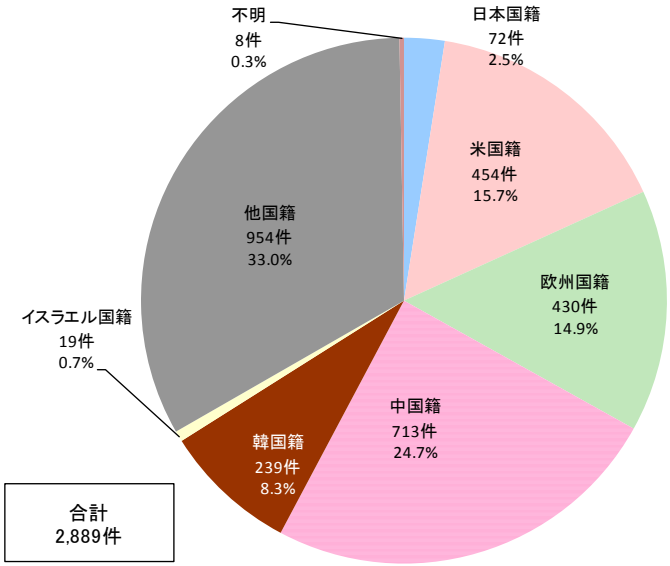


表 5-1
Web of Science における、論文発行主体件数ランキング

順位	論文発行主体/学会等	件数
1	IEEE ELECTRICAL ELECTRONICS ENGINEERS INC	354
2	SPRINGER	319
3	ELSEVIER SCIENCE B.V.	292
4	WILEY-BLACKWELL	178
5	IEEE COMPUTER SOCIETY	117
6	HINDAWI PUBLISHING CORPORATION	94
7	PERGAMON-ELSEVIER SCIENCE LTD	87
8	ASSOCIATION FOR COMPUTING MACHINERY	86
9	ELSEVIER ADVANCED TECHNOLOGY	75
10	INSTITUTE OF ELECTRONICS, INFORMATIO and COMMUNICATINO ENGINIEERS	74

第２節　技術区分別動向調査・分析

技術区分別論文発表件数についてみると、侵入検知分野の IPS/IDS や暗号技術分野の守秘・秘匿のための暗号利用基礎プロトコル、鍵管理、量子鍵配送（単一光子量子技術、単一光子制御）に関わる論文の発表件数が多い。このうち、IPS/IDS は米国籍、欧州国籍、中国籍の研究者所属機関による論文が多い。また、守秘・秘匿のための暗号利用基礎プロトコルについては、米国籍、中国籍の研究者所属機関による論文が多く、量子鍵配送（単一光子量子技術、単一光子制御）については、欧州国籍、中国籍の研究者所属機関による論文が多くなっている。これらの分野は、近年、国際的な技術開発・研究開発競争が激しくなっているものと考えられる。

第３節　研究者所属機関・研究者別動向調査・分析

研究者所属機関別論文発表件数のランキングを以下に示す。最も論文の発表件数が多い研究者所属機関は、中国の北京郵電大学で 42 件である。次いで、中国に西安電子科技大学、中国の国防技術大学が続いている。

表 5-2
研究者所属機関別論文発表件数上位ランキング

研究者所属機関別論文発表件数		
順位	研究者所属機関等	論文発表件数
1	Beijing Univ Posts & Telecommun(中国)	42
2	Xidian Univ(中国)	34
3	Natl Univ Def Technol(中国)	30
4	Natl Taiwan Univ Sci & Technol(台湾)	28
5	Shanghai Jiao Tong Univ(中国)	28
6	Korea Univ(韓国)	27
7	Indian Inst Technol(インド)	26
8	Natl Taiwan Univ(台湾)	26
9	Nanyang Technol Univ(シンガポール)	22
10	Wuhan Univ(中国)	22
11	Natl Cheng Kung Univ(台湾)	21
12	Univ Elect Sci & Technol China(中国)	21
13	King Saud Univ(サウジアラビア)	20
14	Chinese Acad Sci(中国)	19
15	Kyungpook Natl Univ(韓国)	18
16	Univ Waterloo(カナダ)	18
17	Zhejiang Univ(中国)	18
18	Beijing Jiaotong Univ(中国)	17
19	Huazhong Univ Sci & Technol(中国)	17
20	Natl Chiao Tung Univ(台湾)	17
21	Univ Sci & Technol China(中国)	17
22	Dalian Univ Technol(中国)	16
23	Tsinghua Univ(中国)	16
24	Michigan State Univ(アメリカ)	15
25	Natl Chung Hsing Univ(台湾)	14
26	Sungkyunkwan Univ(韓国)	14
27	Chongqing Univ(中国)	13
28	Harbin Inst Technol(中国)	13
29	Natl Tsing Hua Univ(台湾)	13
30	Texas A&M Univ(アメリカ)	13
31	Xi An Jiao Tong Univ(中国)	13
32	Natl Sun Yat Sen Univ(台湾)	12
33	Peking Univ(中国)	12
34	Virginia Tech(アメリカ)	12

第４節　注目論文の変遷の調査・分析

2009 年から 2014 年までの期間において、各年別に最も被引用回数が多かった論文とその概要を以下の表に示す。合計 6 つの論文のうち、4 つが QKD(Quantum Key Distribution、量子鍵配送)に関する論文である。

表 5-3
各年別の最も被引用回数が多い論文とその概要

発刊年	被引用回数	資料名	論文名	研究者所属機関	論文概要
2009	126	NEW JOURNAL OF PHYSICS	The SECOQC quantum key distribution network in Vienna	Austrian Inst Technol GmbH(オーストリア)	SECOQC(Secure Communication based on Quantum Cryptography、量子暗号によるセキュアな通信システムの構築を目指すプロジェクト)による、QKD（Quantum Key Distribution, 量子鍵配送）ネットワーク関連研究の総論。
2010	261	NATURE NANOTECHNOLOGY	A diamond nanowire single-photon source	Harvard Univ(アメリカ)	ダイヤモンドナノワイヤ中の窒素空孔を利用した単一光子源による量子暗号通信に関する論文。
2011	152	OPTICS EXPRESS	Field test of quantum key distribution in the Tokyo QKD Network	Natl Inst Informat & Commun Technol(日本)	6つの異なるQKDにより構成されている統合型システムの、首都圏におけるフィールドテストの報告に関する論文。
2012	69	JOURNAL OF MEDICAL SYSTEMS	A Secure Authentication Scheme for Telecare Medicine Information Systems	Natl Taiwan Univ(台湾)	テレケア医療情報システムにおけるデータの整合性、機密性、可用性保持のための安全かつ実用的な認証に関する論文。
2013	72	NATURE PHOTONICS	Experimental demonstration of long-distance continuous-variable quantum key distribution	Telecom ParisTech(フランス)	光ファイバを利用した、80km以上の環境下における、長距離連続変数QKDの実験証明に関する論文。
2014	31	PHYSICAL REVIEW LETTERS	Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution	Univ Toronto(カナダ)	全ての測定器サイドのチャネル攻撃の影響をうけない、偏光エンコーディング測定装置無依存QKDの実験証明に関する論文。

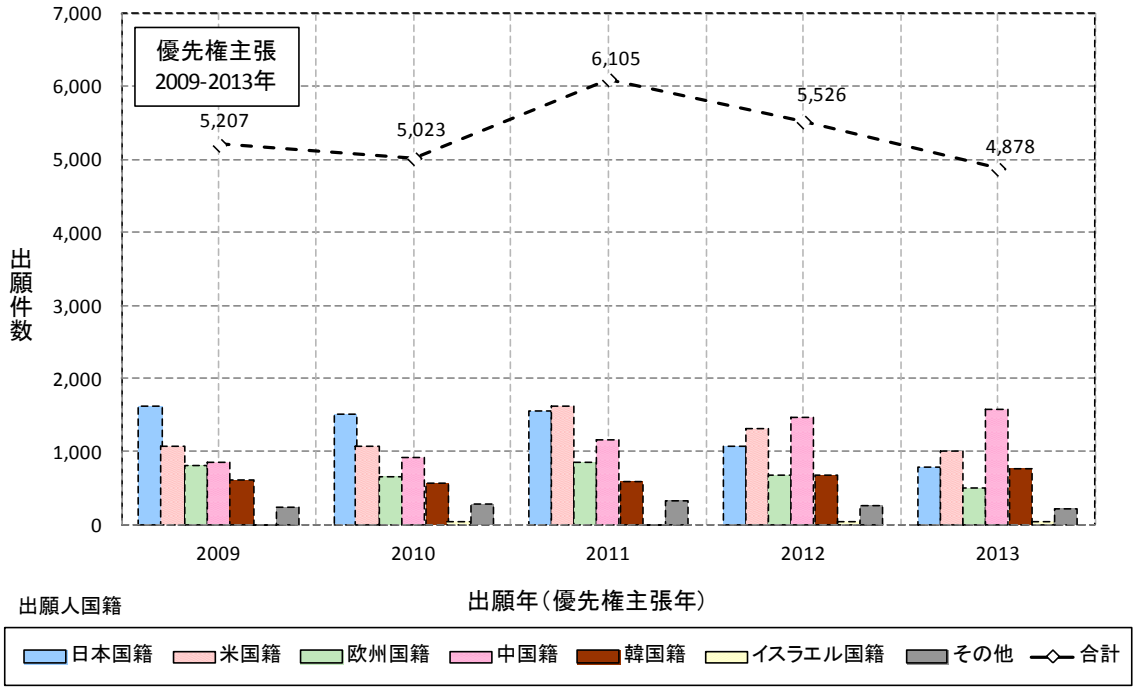
第６章　総合分析と提言

第１節　技術開発競争や市場競争に関しての現状

１．技術開発競争に関しての現状

技術開発競争に関しての現状を分析するため、出願人国籍別出願件数推移についてみると、日本国籍の出願人による出願件数は、欧州国籍の出願人による出願件数や韓国籍の出願人による出願件数と共に、ほぼ横ばいの状態である。他方、米国籍、中国籍の出願人による出願件数は増加傾向が見られる。2011 年時点で日本国籍の出願人による出願件数は、米国籍の出願人による出願件数に追い抜かれ、首位の座を明け渡している。

図 6-1
出願人国籍別出願件数推移



注）2012年以降は、データベース収録の遅れ、PCT出願の各国移行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。

このような結果は、情報セキュリティ分野に携わる日本国籍の出願人において、革新的な製品・ツールの技術開発・研究開発を軽視する姿勢が強まってきていることの表れであり、国内技術や国内製品・ツールの空洞化の進展が現実味を帯びつつあると考えられる。

他方、米国籍、中国籍の出願人について、第４部の注目出願人の調査・分析で挙げているプレイヤーの技術区分別の出願件数推移についてみると、IBM（米国）では、侵入検知やウイルス・マルウェア検知の予防・抑制（侵入・異常対策）といった技術分野や、IT システムが扱う情報のセキュリティ向上のための検知精度の向上、漏えい危険性の低下、不正利用防止といった課題分野の出願件数が件数を大幅に伸ばしている。また、INTEL（米国）では、ブロック暗号やハッシュ関数、暗号利用基礎プロトコルとしての守秘・秘匿、鍵管理、鍵生成といった暗号技術分野や、IT システムが扱う情報のセキュリティ向上のための漏えい危険性の低下、不正利用防止、認証精度・安全性向上といった課題分野、セキュアなデバイスやセキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。主要な米国企業における技術開発競争としては、巧妙化・複雑化する攻撃手法への対策やそれらの攻撃から情報を守るための対策が中心となっている。

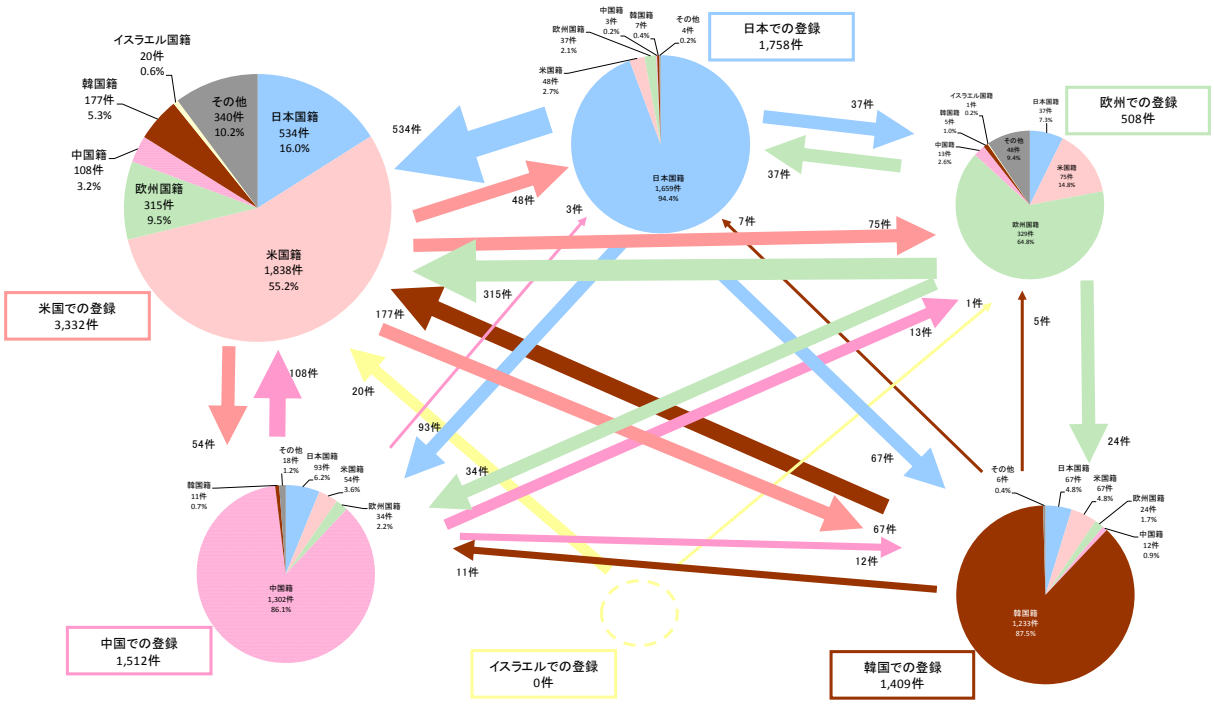
他方、ZTE（中国）では、鍵生成や SIM カードといった技術分野や、IT システムが扱う情報のセキュリティ向上のための漏えい危険性の低下、認証精度・安全性向上といった課題分野、セキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。また、TENCENT TECHNOLOGY SHENZHEN（中国）では、

ウイルス・マルウェア検知の予防・抑制（侵入・異常対策）としてのウイルス対策や検知・判定手法としてのパターンマッチング手法、回復アクション、顔認証といった技術分野や、IT システムが扱う情報のセキュリティ向上のための検知精度の向上、認証精度・安全性向上といった課題分野、セキュアなモバイルコンピューティングといった適用領域・用途分野の出願件数が件数を大幅に伸ばしている。主要な中国企業における技術開発競争としては、ウイルス・マルウェアへの対策やそれらの攻撃から情報を守るための対策、生体認証、モバイルコンピューティング分野のセキュリティ向上が中心となっている。

２．市場競争に関しての現状

市場競争に関しての現状を分析するため、出願先国別－出願人国籍別登録収支についてみると、日本国籍の出願人や欧州国籍の出願人による米国への登録件数がそれぞれ 534 件、315 件と比較的多いものの、それを除くと全体的にみて自国での登録が圧倒的に多く、他国への登録は低調である。

図 6-2
出願先国別－出願人国籍別登録件数収支



このような結果は、米国を除く、日欧中韓イスラエル５極における情報セキュリティ技術分野の市場が閉鎖的であることだけでなく、自国市場において一定規模の市場が形成されていることの表れであり、自国市場は比較的安定的であり、海外市場開拓においては市場競争がこれまで以上に厳しさを増してきていると考えられる。

日本の企業のうち、第４部の出願先国別－出願人別出願件数上位ランキング（全体）の米欧中韓イスラエルへの出願において 20 位以内にランキングしているのは、東芝、富士通、ソニー、日本電気、キヤノン、三菱電機、日本電信電話の７社のみであり、日本企業の海外市場での競争力は必ずしも十分に優位であるとは言えない状況である。

３．総合分析

上記１および２で見てきたように、日本企業における現状の技術開発競争や市場競争はかなり低調である。国内市場の安定性や海外市場開拓の難しさがこの傾向に一層の拍車をかけるおそれもある。

こうした状況のもとで、ログ解析、リバースエンジニアリング分野の UBIC のように、同分野での出願人別出願件数上位ランキング（技術区分別）の上位に入り、日本のみならず米欧中韓への出願にも積極的で、海外市場開拓・拡大を見据えたベンチャー企業が台頭する動きもみられる。

図 6-3
ログ解析、リバースエンジニアリング分野における米欧中韓への出願における
出願人別出願件数上位ランキング

【米国への出願】

順位	出願人名	出願件数
1	IBM(米国)	46
2	SYMANTEC(米国)	16
3	KASPERSKY LAB STOCK(ロシア)	11
3	HEWLETT-PACKARD DEV(米国)	11
5	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE(韓国)	9
5	TENCENT TECHNOLOGY SHENZHEN(中国)	9
7	RAYTHEON (米国)	8
8	VERISIGN(米国)	7
9	UBIC	6
10	MICROSOFT(米国)	5
10	MICROSOFT TECHNOLOGY LICENSING (米国)	5
10	MCAFEE(米国)	5
10	JUNIPER NETWORKS(米国)	5
14	FORTINET(米国)	4
14	INTEL(米国)	4
14	BANK OF AMERICA(米国)	4
14	BOEING(米国)	4
18	EMC(米国)	3
18	LOOKOUT(米国)	3
18	F SECURE(欧州)	3
18	AHNLAB(韓国)	3
18	MITSUBISHI ELECTRIC	3

【欧州への出願】

順位	出願人名	出願件数
1	KASPERSKY LAB STOCK(ロシア)	10
2	IBM(米国)	9
3	VERISIGN(米国)	5
3	HEWLETT-PACKARD DEV(米国)	5
5	UBIC	4
6	BOEING(米国)	3
6	JUNIPER NETWORKS(米国)	3
6	EVIDENCE TALKS(欧州)	3
6	RAYTHEON (米国)	3
6	F SECURE(欧州)	3
11	TENCENT TECHNOLOGY SHENZHEN(中国)	2
11	INTEL(米国)	2
11	OBERTHUR TECHNOLOGIES(欧州)	2
11	GIESECKE & DEVRIENT(欧州)	2
11	SEVEN NETWORKS(米国)	2

注）順位16 位以降は、出願件数1件の出願人が多数存在する。

【中国への出願】

順位	出願人名	出願件数
1	TENCENT TECHNOLOGY SHENZHEN(中国)	17
2	BEIJING QIHOO SCI & TECHNOLOGY(中国)	11
3	BEIJING JINSHAN NETWORK TECHNOLOGY(中国)	7
4	BEIJING ANTIY ELECTRONIC APPLIANCE(中国)	5
4	IBM(米国)	5
4	HEWLETT-PACKARD DEV(米国)	5
7	KASPERSKY LAB CLOSED(ロシア)	4
7	UBIC	4
9	SIEMENS(欧州)	3
9	UNIV NANJING POSTS & TELECOM(中国)	3
9	IBM(中国)	3
9	ZHUHAI KINGSOFT(中国)	3
9	BAIDU ON-LINE NETWORK TECHNOLOGY(中国)	3
9	HARBIN ANTIY TECHNOLOGY(中国)	3
9	INST SOFTWARE CHINESE ACAD SCI(中国)	3
9	UNIV BEIJING POSTS & TELECOM(中国)	3
9	JUNIPER NETWORKS(中国)	3
9	UNIV NAT DEFENSE TECHNOLOGY(中国)	3
9	ZHUHAI JUNTIAN ELECTRONIC TECHNOLOGY(中国)	3
9	TENCENT SHENZHEN(中国)	3

【韓国への出願】

順位	出願人名	出願件数
1	ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE(韓国)	17
2	KOREA INTERNET & SECURITY AGENCY(韓国)	14
3	INCA INTERNET(韓国)	5
3	AHNLAB(韓国)	5
5	UBIC	4
6	INTEL(米国)	2
6	REPUBLIC KOREA SUPREME PUBLIC PROSECUTOR(韓国)	2
6	PANTECH(韓国)	2
6	SK TELECOM(韓国)	2
6	UNIV SOONCHUNHYANG IND ACAD COOP FOUNDA(韓国)	2
6	HEWLETT-PACKARD DEV(米国)	2
6	UNIV HANYANG IUCF-HYU(韓国)	2
6	UNIV KOREA RES & BUSINESS FOUND(韓国)	2
6	KT(韓国)	2
6	UNIV SUNGSHIN WOMENS IND ACAD COOP FOUND(韓国)	2
6	WINS TECHNET(韓国)	2
6	MCAFEE(米国)	2

注）順位18位以降は、出願件数1件の出願人が多数存在する。

今後は日本において、UBIC のようなベンチャー企業が数多く輩出されることが、技術開発競争や市場競争の活性化の大きな起爆剤になるものと考えられる。

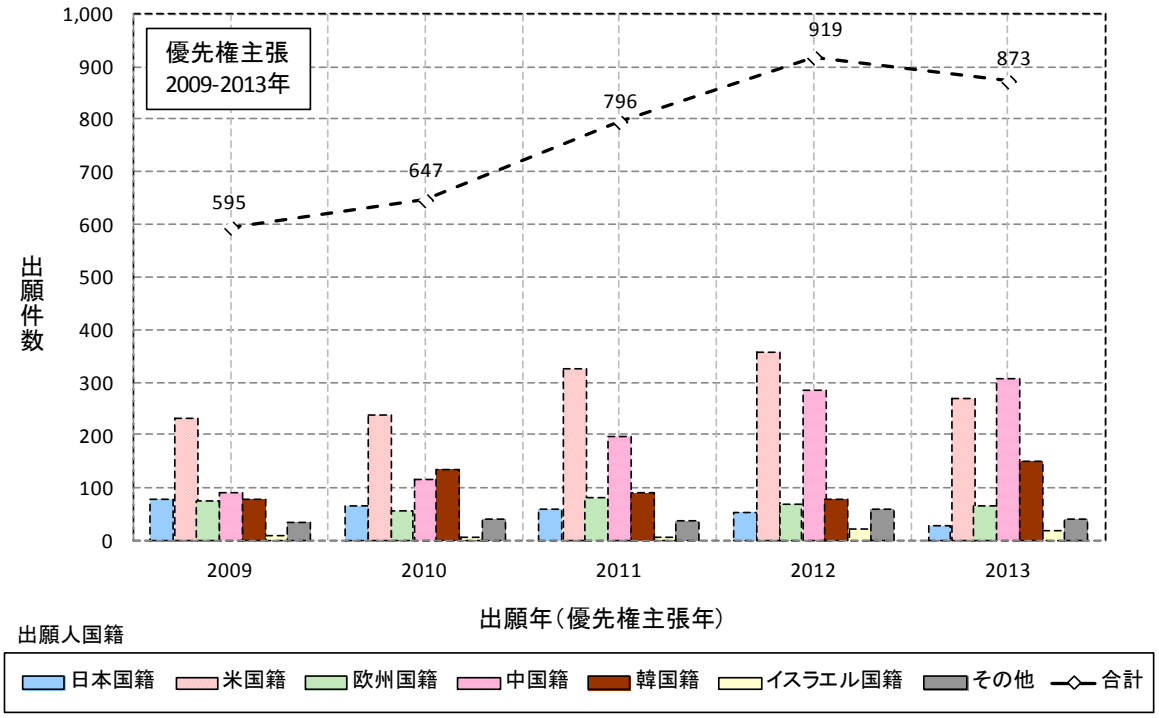
第２節　将来の技術開発や市場

１．将来の技術開発

将来の技術開発に関して分析するため、技術区分別－出願人国籍別出願件数推移についてみると、近年出願件数を大幅に伸ばしているのが、ウイルス・マルウェア検知とログ解析である。

ウイルス・マルウェア検知においては、日本国籍の出願人による出願件数は 2009 年から 2011 年にかけて減少傾向である。他方、米国籍の出願人や中国籍の出願人による出願件数は、2009 年から 2012 年にかけて、件数を大幅に伸ばしてきている。

図 6-4
ウイルス・マルウェア検知における出願人国籍別出願件数推移



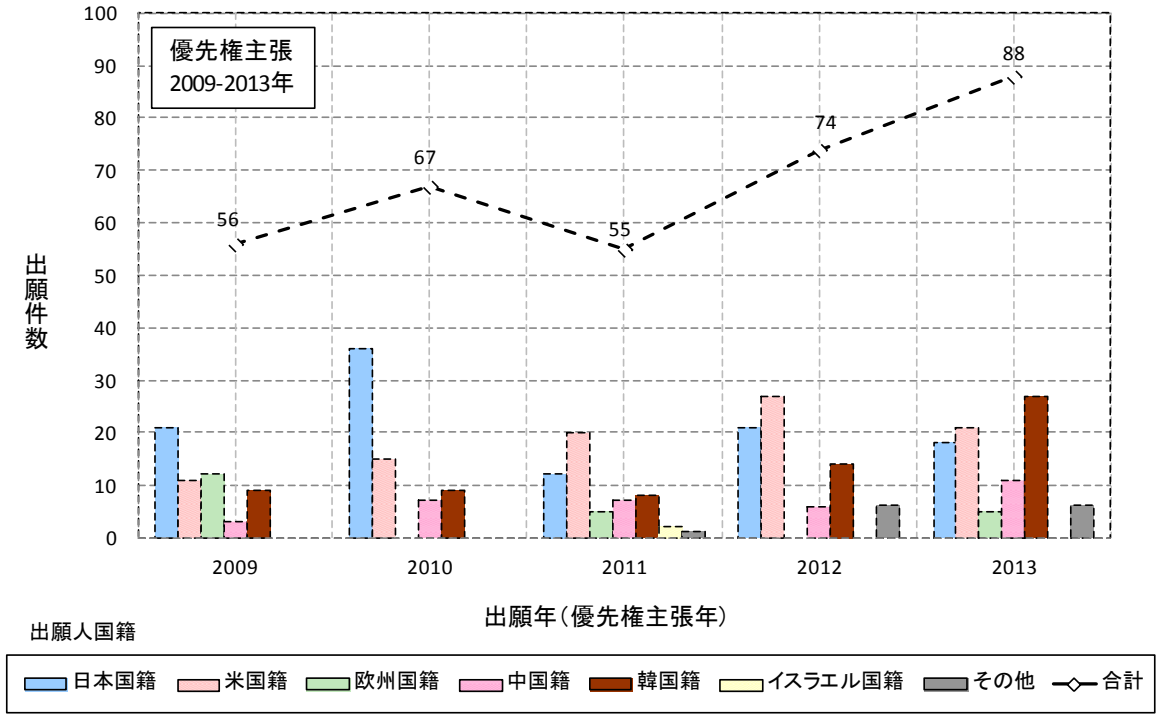
注）2012年以降は、データベース収録の遅れ、PCT出願の各国移行のずれ等で全出願データを反映していない可能性がある。

このような結果は、ウイルス・マルウェアによる攻撃手法が巧妙化・複雑化する中で、攻撃に対して通用しない検知・判定手法が増えてきて、検知・判定手法の更なる高度化が必要になっていることの表れである。ウイルス・マルウェア検知における技術区分別出願件数推移についてみると、検知・判定手法としては、ブラックリスト・ホワイトリストを用いたパターンマッチング手法の出願件数が件数を比較的伸ばしている。また、静的ヒューリスティック手法の出願件数は減少傾向にあるのに対し、動的ヒューリスティック手法の出願件数は増加傾向にある。さらに、それらの手法以外によるその他の検知・判定手法についても、出願件数を大幅に伸ばしている。

このような状況から、ウイルス・マルウェア検知の検知・判定手法に関わる技術開発については、今後も攻撃者側と対策者側との間の技術開発競争が継続され、将来には、導入効果が高い新しいウイルス・マルウェア検知・判定手法が登場してくることが予想される。

他方、ログ解析においては、日本国籍の出願人による出願件数は、2009 年の 21 件から 2010 年には 36 件と件数を大きく伸ばしたが、2011 年以降は減少に転じている。他方、米国籍の出願人による出願件数は、2011 年に日本国籍の出願人による出願件数を追い抜き、首位の座に就いたが、2013 年に中国籍の出願人による出願件数に追い抜かれ、首位の座を明け渡している。

図 6-5
ログ解析における出願人国籍別出願件数推移



注）2012年以降は、データベース収録の遅れ、PCT出願の各国移行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。

このような結果は、各国が当該技術分野の技術開発にしのぎを削っていることの表れである。ログ解析における技術区分別出願件数推移についてみると、2009 年から 2011 年、2012 年にかけて出願件数を大きく伸ばしているのは、攻撃者検知や脅威レベルの判定、イベント情報といった技術区分となっている。監視インシデントや監視ログの対象は、これまで中心であった異常通信検知やアプリケーションログ等から、攻撃者検知や脅威レベルの判定、イベント情報へと拡大してきており、このような状況から、将来発生しうる攻撃等が高い確度で予測できるようになる一方、人手による運用の負荷がこれまで以上に高まっていくことが懸念される。

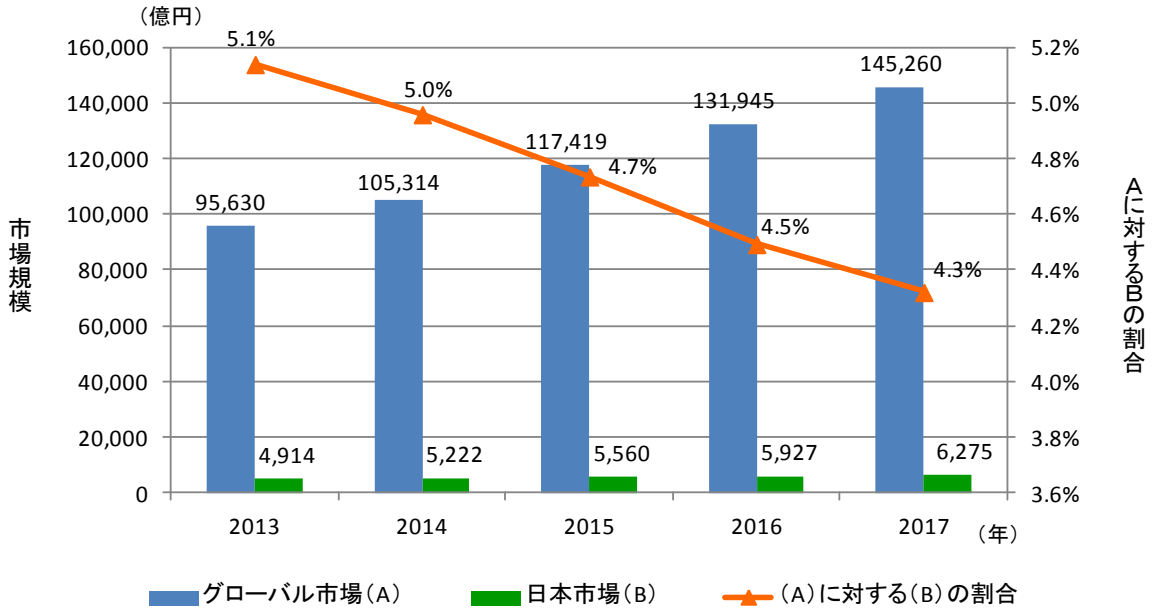
このため、今後はログ解析の効率的な運用を行うために、自動化や人手による運用の負荷軽減のための技術開発が進展していくことが予想される。

２．将来の市場

将来の市場に関して分析するため、情報セキュリティ技術分野のグローバル市場動向についてみると、グローバル市場の規模は、2015 年に 970 億 US ドルであったものが、2017 年には 1,200 億 US ドルに達するものと見込まれている（2015～2017 年の CAGR は 11.2%）。他方、情報セキュリティ技術分野の日本市場動向についてみると、日本市場の規模は、2015 年に 5,560 億円であったものが、2017 年には 6,275 億円に達するものと見込まれている（2015～2017 年の CAGR は 6.2%）。

日本市場のグローバル市場に占める割合は、約 4～5%であり、また、日本市場の成長率はグローバル市場の成長率の半分強であることから、日本市場の相対的な魅力は今後次第に低下傾向が予想されている。

図 6-6
情報セキュリティ技術分野のグローバル市場と日本市場の比較



注）グローバル市場の市場規模は、2016 年 1 月 30 日時点の為替レート（1 ドル＝121.05 円）を基に、日本円に換算している。

出所）Alix Partners Web site および野村総合研究所「IT ナビゲーター2016 年度版」をもとに野村総合研究所作成

このような状況のもとで、日本国籍の出願人が将来の市場として期待を寄せているのが、重要インフラや自動車、住宅、情報家電といった適用領域・用途における情報セキュリティ技術分野の市場である。これらの適用領域・用途では、これまでネットワークに接続されていなかったさまざまな機器がネットワークに接続される IoT（Internet of

Things）を活用して、新たなビジネスの創造や業務の効率化、コスト削減等に繋げるための取組みにおいて、グローバルでの技術開発競争や市場競争が激しくなりつつある。重要インフラや自動車、住宅、情報家電といった産業分野は、日本が強みを有する産業分野であり、このような産業分野での国際競争力の更なる向上を図っていくうえで、IoTを活用した制御系システムや各種機器の組込みソフトウェア等において適用できるようなセキュリティ確保を実現することが重要かつ必要不可欠になってきている。

しかしながら、適用領域・用途における技術区分別－出願人国籍別出願件数についてみると、日本国籍の出願人は、米欧中韓イスラエルの国籍の出願人と比較して、重要インフラや自動車、住宅、情報家電の保護に関わる出願件数がやや多いが、米欧中韓イスラエルの国籍の出願人を圧倒し、日本の競争優位性の確立に繋がるほどの量的にまとまった特許出願が十分なされていないのが現状である。

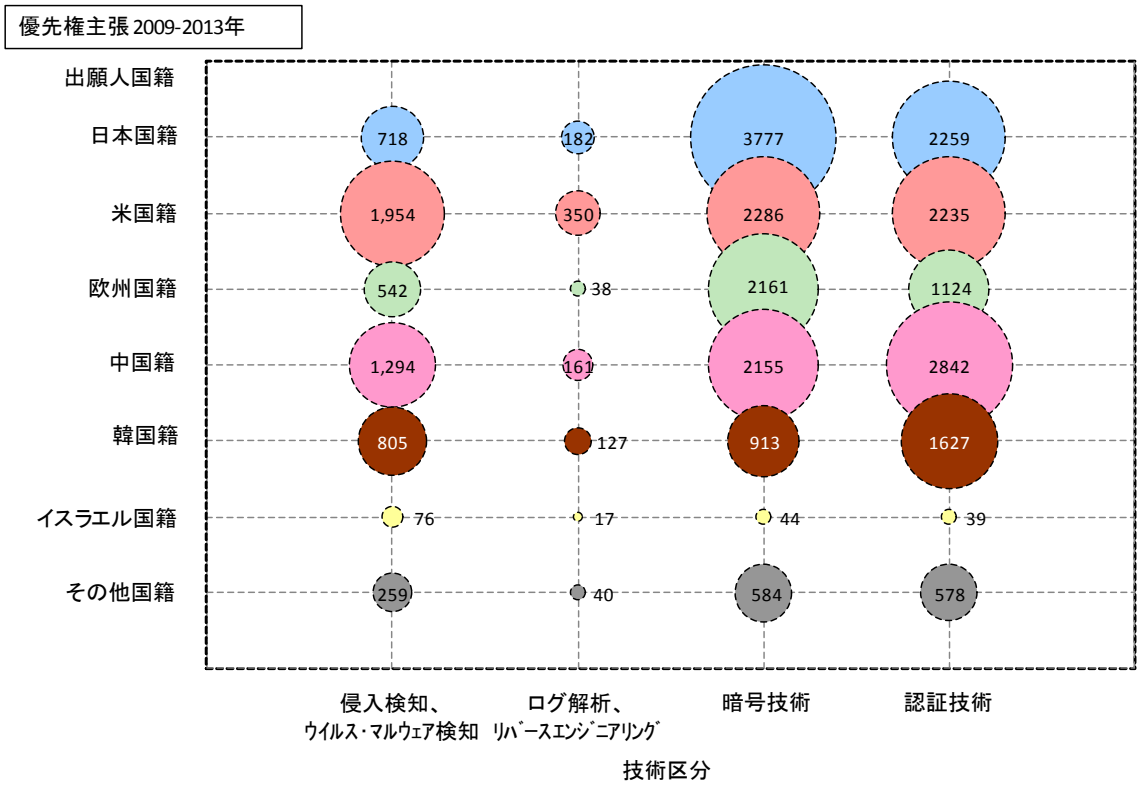
IoT を活用した制御系システムや各種機器の組込みソフトウェア等に適用可能な情報セキュリティ技術が切り拓く市場は今後大きな進展が予想されることから、日本の情報セキュリティ技術分野の市場の魅力低下への歯止めや、重要インフラや自動車、住宅、情報家電といった日本が強みを有する産業分野での更なる国際競争力向上が求められる中で、日本がこの分野の技術開発競争や市場競争で優位性を発揮でき、このような将来の市場を適切に取り込むことができるかどうかが重要な鍵を握っている。

３．総合分析

上記１および２で見てきたように、将来の技術開発や市場においては、ソーシャルエンジニアリング手法の駆使など巧妙化・複雑化する攻撃手法に対する継続的な対策技術の開発と、重要インフラや自動車、住宅、情報家電といった日本が強みを有する産業分野での更なる国際競争力向上の後押しに繋がる IoT を活用した制御系システムや各種機器の組込みソフトウェア等に適用可能な情報セキュリティ技術の開発および関連市場の獲得の２点が重要なポイントになっている。

前者に関しては、技術区分別－出願人国籍別出願件数を見る限り、情報セキュリティ技術分野における日本国籍の出願人による特許出願の特徴として、暗号技術や認証技術に関わる特許出願への偏重傾向が浮き彫りになっている。そのような結果や、巧妙化・複雑化する攻撃手法に対する継続的な対策技術開発の必要性を踏まえると、侵入検知、ウイルス・マルウェア検知やログ解析、リバースエンジニアリングといった情報セキュリティ技術についても、暗号技術や認証技術とほとんど遜色がないレベルで特許出願が可能となるよう技術開発の強化をより一層強力に推進していく必要がある。

図 6-7
技術区分別－出願人国籍別出願件数



また、後者に関しては、IoT を活用した制御系システムや各種機器の組込みソフトウェア等のセキュリティ確保に対応できる日本のプレイヤーが限定的であることが、当該分野での情報セキュリティ技術の開発および関連市場の獲得を進めるうえで障壁となっている。

そもそも国内に、IoT を活用した制御系システムや各種機器の組込みソフトウェア等やそれらに必要なセキュリティの分野に精通している技術者が少ない点が大きな課題である。その影響は、セキュリティを専業とするベンダーの中に、重要インフラや自動車等の分野で求められるセキュリティを理解したうえで有用な提案可能なベンダーが少ないという形になって表れており、重要インフラや自動車等の関連企業においては、競争環境が構築できずコスト圧縮や技術革新に十分対応できない事態を招くことが懸念されている。(大手電力会社および大手自動車メーカーへのヒアリング結果より)

今後、日本において、重要インフラや自動車等の関連企業と、情報セキュリティ技術に携わる企業等の双方が一堂に会して、IoT を活用した制御系システムや各種機器の組込みソフトウェア等に求められるセキュリティに関して議論できるような場を十分確保していくことが、制御系システムのセキュリティ等に対する双方の理解の溝を埋めるとともに、将来の技術開発をリードし、将来の市場を獲得していくうえで重要になるものと考えられる。

第３節　技術開発競争や市場競争に関しての展望

１．技術開発競争に関しての展望

技術開発競争に関しての展望を分析するため、有識者ヒアリングの結果を分析すると、情報セキュリティ技術の開発者・提供者側では、以下のような要素が今後の競争の源泉になると見ている。

①未知の攻撃などに適用可能で、かつ現在の市場に存在しない新しいセキュリティの概念やアーキテクチャを持つ攻撃防御技術

②異常検知やリスク検知のための人工知能技術（AI）を活用した高度なログ解析技術と攻撃防御技術への応用

③アプリケーション領域に適用可能な暗号利用応用プロトコル

上記①に関しては、侵入検知・防御やウイルス・マルウェア検知・防御といった情報セキュリティ技術分野は、長年にわたって攻撃者側と対策者側との間で激しい技術開発競争が繰り広げられてきた経緯があり、攻撃や対策等に関する技術力や知見・ノウハウの蓄積量の多寡が、ビジネス成功の秘訣となっている。そのような観点に基づくと、当該分野での技術開発競争に関しては、グローバル市場でビジネスを展開する米国を中心とする海外のセキュリティベンダーが優位なポジションを築くことが避けられない状況となっている。今後もこのような傾向は続くものと予想されるが、日本のセキュリティベンダーが存在感を高めていくためには、蓄積量との直接的な関係性が高くない新技術分野において活路を見出すことが重要であり、既に先行するFFRIが標的型攻撃に特化したプログレッシブ・ヒューリスティック技術を開発したように、新しい概念やアーキテクチャを持つ攻撃防御技術を開発していくことが競争優位性の確立に繋がるものと考えられる。またその他に、革新的な技術開発・研究開発のための国際連携の強化や、国主導の下での攻撃や対策等に関する技術力や知見・ノウハウを蓄積する仕組みの構築などといった蓄積量を補うための方策についても競争優位性の確立に繋がるものと考えられる。

また、上記②に関しては、これまでのログ解析においては、主にトラフィックログや、データベースログ、アクセス権限を管理するPCやサーバのログ等を解析対象としていたが、攻撃手法の巧妙化・複雑化が進み、コンプライアンスや内部統制などセキュリティで括られる範囲が広がってきている近年においては、監視カメラの映像ログや、入退管理システムの認証やプリンター出力等の操作ログ、室内環境の温度変化等の環境ログなど多種多様なログを収集し解析対象とする動きが活発化してきている。その一方で、解析作業に関しては、解析対象範囲の広がりに伴い、解析従事者の負担が過重なものとならないように、人工知能技術（AI）を効果的に活用していくことが重要となってきている。今後は、このような人工知能技術（AI）を、異常検知やリスク検知のみならず、攻撃防御にまで応用することができれば、競争優位性の確立に繋がるものと考えられる。

さらに、上記③に関しては、第４部の暗号技術における技術区分別－出願人国籍別出願件数で前述したとおり、日本国籍の出願人は、暗号プリミティブや暗号利用基礎プロトコルに関わる技術、さらに暗号利用応用プロトコルのうち、秘密分散・秘密計算や量

子暗号通信といった技術において、米欧中韓イスラエルの国籍の出願人よりも出願件数が相対的多くなっており、優位なポジションを獲得している。暗号技術分野の技術開発は直ちにビジネスに繋がらないものの、新たな産業創出の種となるものであることから、アプリケーション領域にフォーカスしつつ、今後も適用可能な暗号利用応用プロトコルを開発していくことが競争優位性の確立に繋がるものと考えられる。

他方、IoT を活用した制御系システムや各種機器の組込みソフトウェア等に適用可能な情報セキュリティ技術の利用者側では、以下のような要素の技術開発競争を望んでいる。

①一般の PC や企業等の事務処理系情報システムのセキュリティとは異なる、新しい概念やアーキテクチャを持つ情報セキュリティ技術

②海外市場での事業展開において適用可能な情報セキュリティ技術

上記①に関しては、一般の PC や企業等の事務処理系情報システムと IoT を活用した制御系システム等を比較した場合に、情報セキュリティ技術を実装する際の制約条件が大きく異なる点に対して、十分考慮する必要がある。具体的には、各種機器側のリソース上の制約や各種計算処理にかかる応答性の制約、ジャミング等の妨害行為への対応上の制約などが課題として挙げられ、それらをどう克服できるかが重要となる。今後は、各種機器側への負荷がかからず、高いセキュリティが確保された新しい暗号技術を開発するなど、課題を解決するための技術を開発していくことが、競争優位性の確立に繋がるものと考えられる。

上記②に関しては、取り分け、自動車のような産業分野では、海外市場での事業展開・拡大に重点を置いた対応が基本となっており、情報セキュリティ技術の実装においても、この対応の考え方は一様に適用される。今後は、国際標準の獲得を視野に入れつつ、海外市場での事業展開において適用可能な情報セキュリティ技術を開発していくことが、競争優位性の確立に繋がるものと考えられる。

２．市場競争に関しての展望

市場競争に関しての展望を分析するため、出願先国別－出願人国籍別登録収支についてみると、日本国籍の出願人においては、米国市場での事業展開のみが比較的良好であるように見える。しかしながら、欧州国籍や韓国籍の出願人においても、米国市場での競争優位性の確立を狙っており、今後、米国のプレイヤーも含めて米国市場の獲得競争は一段と激しさを増すものと考えられる。

他方、中国市場や韓国市場等においては、自国で開発された情報セキュリティ技術の権益を保護する動きが強まっており、日本のプレイヤーによる今後の市場獲得のハードルは一段と高くなるものと考えられる。

このような状況のもとで、今後、市場競争の力点は、日米欧中韓の市場に代表される成熟市場から新興国の未成熟市場へ、また一般の PC や企業等の事務処理系情報システムのセキュリティ市場から IoT を活用した制御系システム等のセキュリティ市場へと移行していくものと考えられる。

情報セキュリティ技術分野のグローバル市場動向についてみると、アジア太平洋地域

の市場が急速に拡大していくことが見込まれており、セキュリティ意識が高い政府機関や重要インフラ関連企業を中心に、このような成長著しい新興国の未成熟市場を取り込むことが、競争優位性の確立に繋がるものと考えられる。

３．総合分析

前述したとおり、日本企業における現状の技術開発競争や市場競争はかなり低調であり、国内市場の安定性や海外市場開拓の難しさがこの傾向に少なからぬ影響を与えている。また今後は、日本の情報セキュリティ技術分野の市場の魅力低下への歯止めや、重要インフラや自動車、住宅、情報家電といった日本が強みを有する産業分野での更なる国際競争力向上が求められるようになる。

このように、情報セキュリティ技術分野に携わる日本のプレイヤーに求められる役割はますます多義的なものとなっており、そのような状況のもとで、新しいセキュリティの概念やアーキテクチャを持つ攻撃防御技術や人工知能技術（AI）を活用した高度なログ解析技術と攻撃防御技術への応用、アプリケーション領域に適用可能な暗号利用応用プロトコルといった既存の情報セキュリティ技術・製品分野の新技術・新製品や、IoTを活用した制御系システム等の分野の新しい概念やアーキテクチャを持つ情報セキュリティ技術が、日本市場活性化や海外市場開拓、さらには日本が強みを有する産業分野での更なる国際競争力向上の突破口になると考えられる。

今後は、上記に示した技術領域における技術開発競争や市場競争がこれまで以上に厳しさを増すものと予想されるが、より高いレベルのセキュリティ品質とリーズナブルな価格受容性の双方を実現していくことが、日本のプレイヤーの競争優位性の確立に繋がるものと考えられる。

第４節　目指すべき研究開発、技術開発の方向性

１．目指すべき情報セキュリティ分野の国産技術・製品の研究開発、技術開発

情報セキュリティ技術分野に携わる日本のプレイヤーに求められる役割がますます多義的なものとなっている中で、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」というセキュリティが果たすべき役割の原点に立ち返った検討が必要とされている。

このうち、我が国の安全保障においては、国家安全保障や重要情報保全に関わる高度なセキュリティ技術やセキュリティ製品・ツールの調達において、セキュリティ保証がコントロールされた自国の国産技術・製品・ツールを採用し導入することが、我が国の国家安全保障や国内の重要情報保全の強化にとって有効な手段と考えられる。

海外においては、政府が自国の軍や大学のセキュリティ技術開発・研究開発に対して積極的な関与や支援を行い、そこで生まれた新しいセキュリティ技術を政府や企業が調達・採用している国が多く見られる。一方、日本においては、そのようなスキームが実装されておらず、政府や企業等の需要側と開発側の双方において、海外と比べて、国産

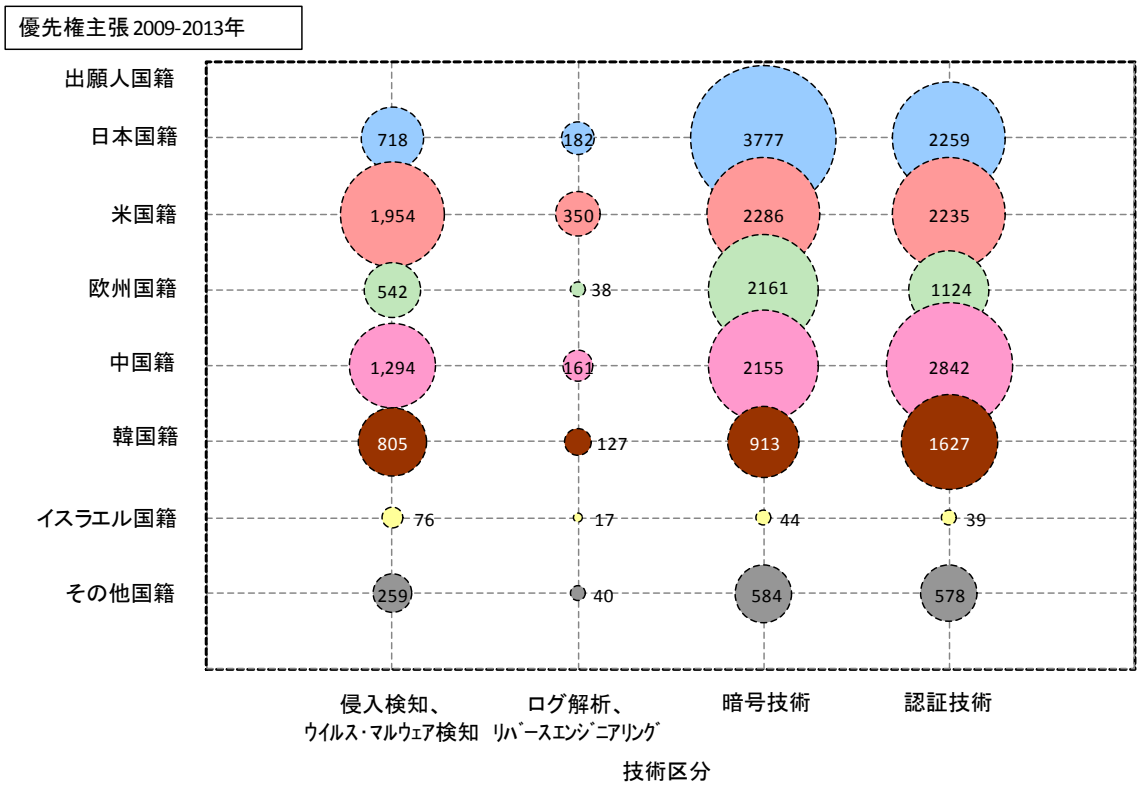
技術・製品・ツールの実装・開発の重要性に対する認識がほとんど浸透していない。

こうした状況のもと、我が国おけるセキュリティ技術開発・研究開発は、国家安全保障や重要情報保全という目的よりも、経済性の目的が優先されがちであり、自社開発にかかるコストと海外からの調達にかかるコストを比べて、その大小により投資の効果が判断される傾向が強まっている。結果として、海外企業の技術等が中心となって国内市場に提供されている状況は同じでも、技術等の分野によって、技術開発・研究開発が進展しているものと、技術開発・研究開発が低調であるものが大きく分かれるなど、情報セキュリティ技術開発・研究開発の分野は、バランスの悪いものとなっている。

技術区分別－出願人国籍別出願件数について見ると、日本国籍の出願人による特許出願の特徴として、暗号技術や認証技術に関する出願件数が、侵入検知、ウイルス・マルウェア検知やログ解析、リバースエンジニアリングに関する出願件数に比べて圧倒的に多くなっている。その傾向は、米国籍や欧州国籍、中国籍、韓国籍の出願人と比較して顕著である。

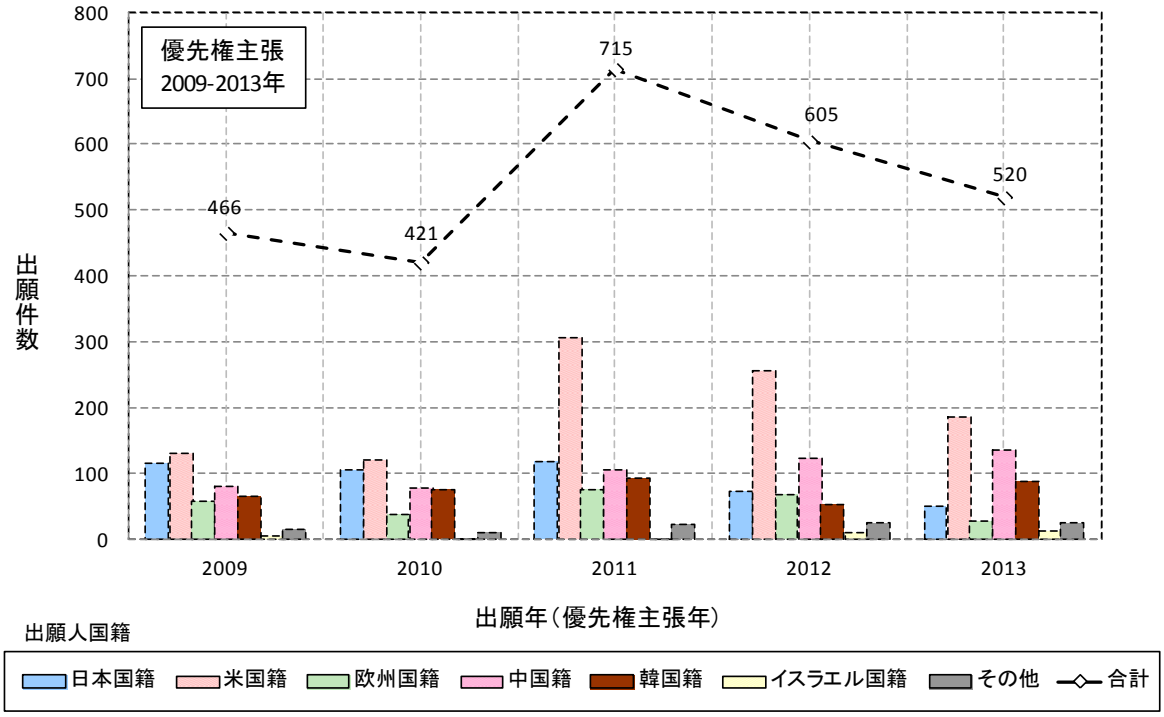
図 6-8

技術区分別－出願人国籍別出願件数



また、技術区分別－出願人国籍別出願件数推移について見ると、侵入検知、ウイルス・マルウェア検知やログ解析に関する出願件数は、米国籍の出願人や中国籍の出願人において、近年、件数が大幅に伸びているが、日本国籍の出願人においては、概ね横ばいか、微減傾向となっている。（ウイルス・マルウェア検知、ログ解析については、図 6-3-1、図 6-3-2 にて前述）

図 6-9
侵入検知における出願人国籍別出願件数推移



注）2012年以降は、データベース収録の遅れ、PCT出願の各国移行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。

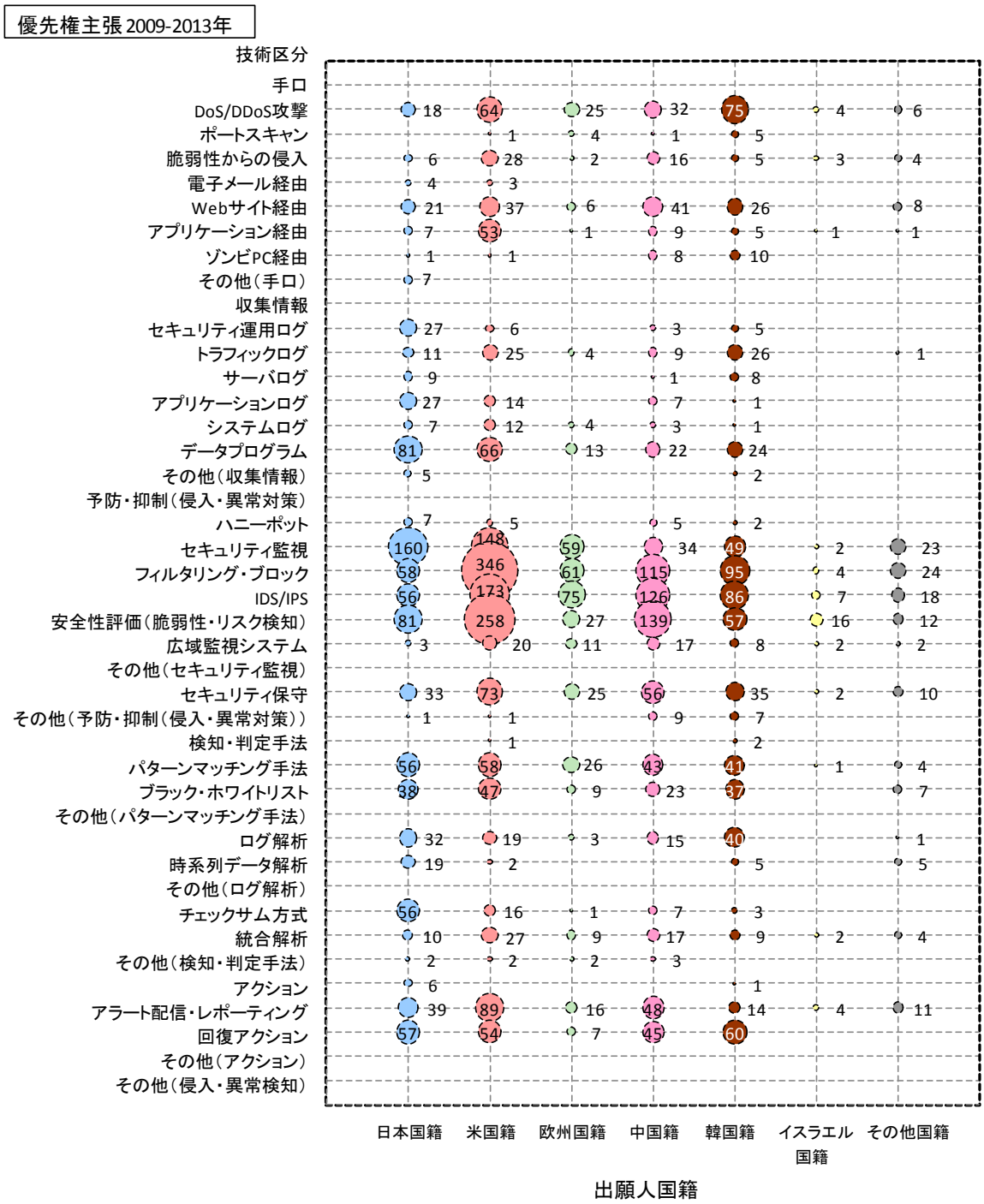
それらの結果を踏まえると、侵入検知、ウイルス・マルウェア検知やログ解析、リバースエンジニアリングといったセキュリティ技術についても、暗号技術等と同様、我が国において強みのある国産技術を開発し保有できるようにすることが、性善説に立って、海外の製品等が検知・解析した情報を信用し、鵜呑みにせざるを得ない状況や、未知の脅威・リスク等を誘発する海外の製品等を仕掛けられる危険性と隣り合わせにある状況等を回避し、我が国の国家安全保障や国内の重要情報保全の強化をより一層強力に推進していく上で重要かつ不可欠である。

他方、侵入検知、ウイルス・マルウェア検知については、予防・抑制対策としての検知精度の向上もさることながら、検知後のアクセス制御やネットワークの分離・遮断、事後対応の準備、攻撃者の追跡等といった回復アクションとしての攻撃防御技術の重要性が指摘されているところである。（大手 IT ベンダーへのヒアリング結果より）

侵入検知、ウイルス・マルウェア検知それぞれにおける技術区分別－出願人国籍別出願件数について見ると、侵入検知の場合は、日本国籍の出願人による出願件数と、米国籍や中国籍、韓国籍の出願人による出願件数との間に有意な差が見られないが、ウイルス・マルウェア検知の場合は、双方の件数に大きな開きがあり、我が国がウイルス・マルウェア検知に関する技術競争力を保有していく上での改善の余地がかなりある。

図 6-10

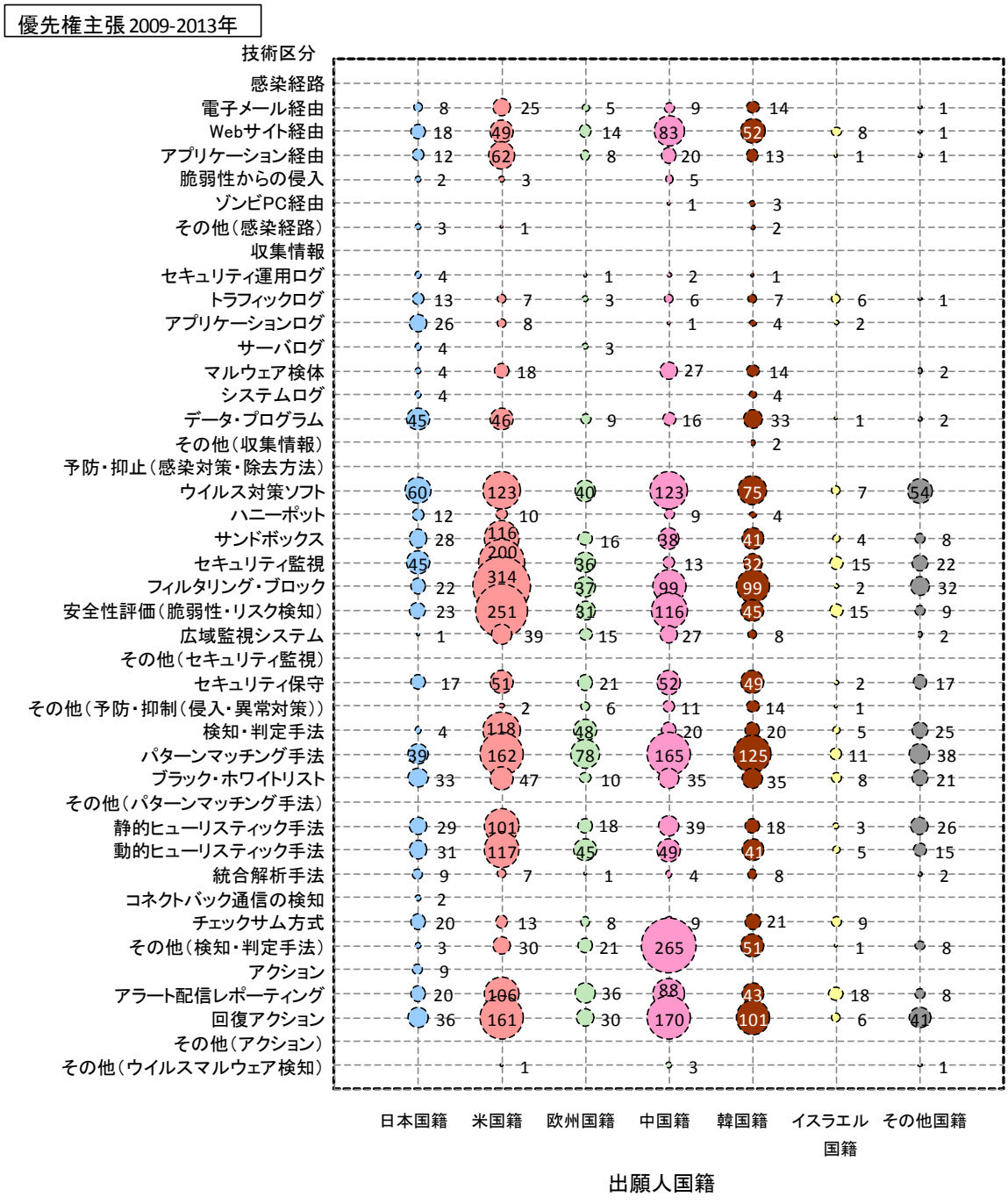
侵入検知における技術区分別－出願人国籍別出願件数



要約

図 6-11

ウイルス・マルウェア検知における技術区分別－出願人国籍別出願件数



２．目指すべき IoT を活用した制御系システム等のセキュリティ分野のグローバル市場に通用する技術・製品の研究開発、技術開発

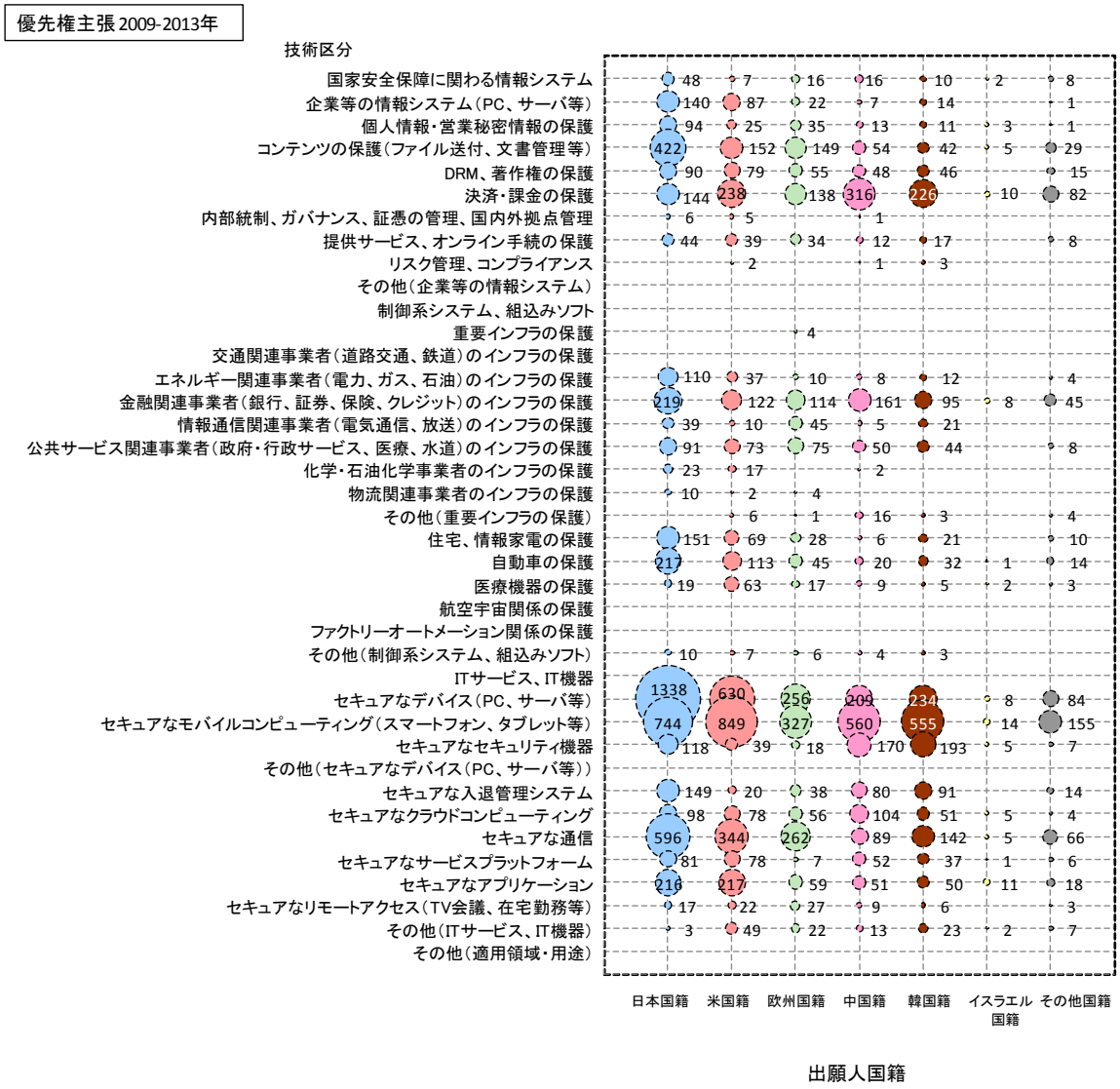
これまでネットワークに接続されていなかったさまざまな機器がネットワークに接続される IoT（Internet of Things）を活用して、新たなビジネスの創出や業務の効率化、コスト削減などの効果を享受し、経済の活力向上をめざす社会が到来しつつある。今後は、自動車や電力関連システムなどの重要インフラにおいても、IoT の活用が進展することが予想されている。

その一方で、IoT を活用する社会においては、新しい攻撃や脅威・リスクが発生することへの危機感・警戒感が強く、そのような攻撃等が人命や経済等に少なからぬ影響を与え、セキュリティ問題の深刻性や複雑性に一層拍車をかけるおそれがある。また、自動車や重要インフラといった産業分野は、日本が国際競争力を有する産業分野であり、セキュリティ対策への対応が遅れることになれば、海外事業展開・拡大に危険信号が灯ることになりかねない状況である。

適用領域・用途における技術区分別－出願人国籍別出願件数について見ると、日本国籍の出願人は、他国籍の出願人と比べて、重要インフラの保護や自動車の保護に関わる出願件数が多く、当該分野のセキュリティに一定の強みが見られるが、こうした強みを更に伸ばし確実なものにしていくうえで、新しいセキュリティアーキテクチャの確立、グローバル市場への対応の両面を持ったセキュリティ技術開発・研究開発を強力に推進し、このような活動を通じて、上記のような懸念を払拭することが重要である。

図 6-12

適用領域・用途における技術区分別－出願人国籍別出願件数



また、韓国では、情報セキュリティ産業発展総合対策という国家戦略を策定し、これからの新成長分野の１つに社会基盤分野を掲げている。この分野には制御システムのセキュリティや社会基盤で扱われる情報のセキュリティが当然含まれているが、注目すべきは、センサーセキュリティモジュールといった末端機器のセキュリティについても成長領域として位置付けていることである。このようなセンサーやコントローラーなどの末端機器の分野は、日本が強みを持つ産業分野であることから、今後そのような分野の市場が韓国などの海外勢に浸食されることがないよう、このような動きに対抗し得るセキュリティ技術・製品等の開発を推進していくことが重要である。

第５節　提言

情報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、情報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るとともに、サイバーセキュリティ戦略が策定され、関係者の共通の理解と行動の基礎が示されている。

また、情報セキュリティ技術分野の研究開発、技術開発については、2014 年 7 月に情報セキュリティ政策会議によって情報セキュリティ研究開発戦略（改定版）が取りまとめられるとともに、内閣府が進める戦略的イノベーション創造プログラム（SIP）においても、重要インフラ等におけるサイバーセキュリティの確保に向けた研究開発が採り上げられている。

本調査が取りまとめる提言の在り方としては、特許出願動向や研究開発動向からみた、我が国が推進する情報セキュリティ政策や情報セキュリティ技術分野の研究開発、技術開発の助言者としての機能を果たす情報提供を行うことを目的とするものである。

（提言１）情報セキュリティ分野の国産技術・製品の技術開発、研究開発にインセンティブを付与すべき

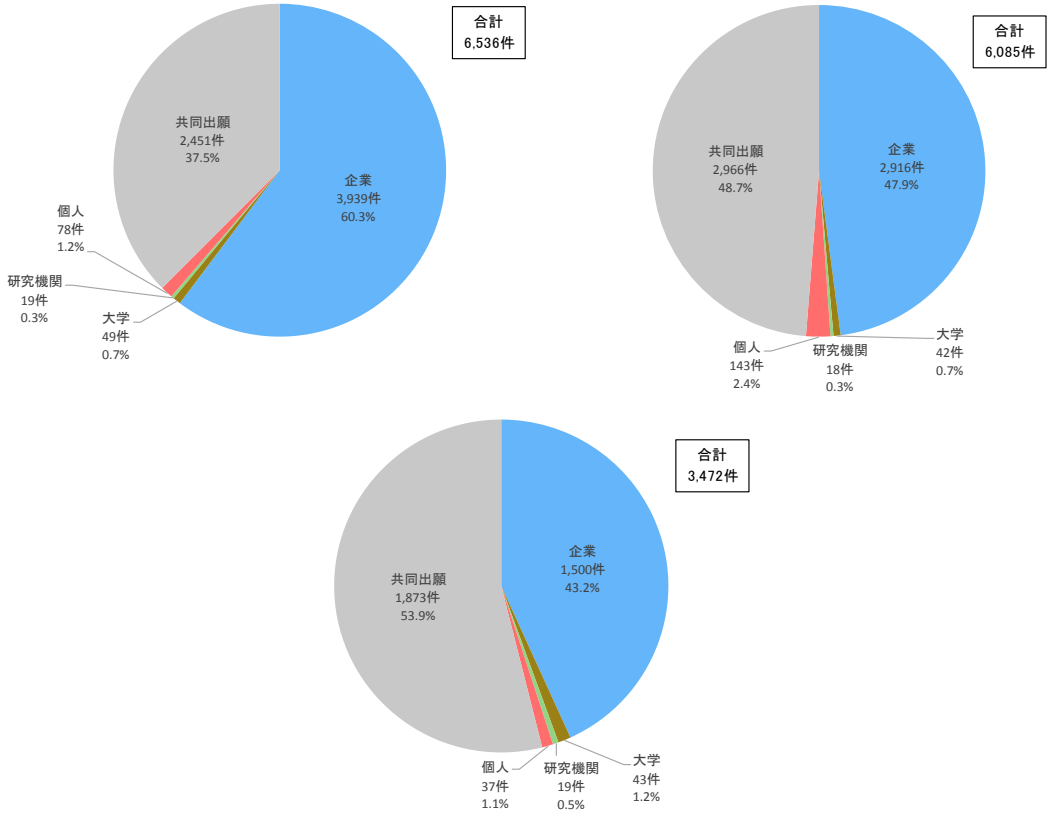
日本のプレイヤーに対して、情報セキュリティ分野の国産技術・製品の技術開発、研究開発に対する積極的な投資を促し、その投資を回収できる仕組み・制度を併せて提示し実装すべきである。

日本のプレイヤーが独自に強みのある国産のセキュリティ技術・製品を開発するうえで課題となるのが投資回収である。課題解決に向けては、開発プロセス自体を効率化する仕組みと、開発される技術等に関して、導入の経済効果が高まる仕組みの２つが必要である。

前者の仕組みについては、セキュリティ分野に携わる政府系研究機関に蓄積されている攻撃等に関するデータや検知、解析業務等のノウハウ等を、信用できるベンチャーなどの企業等に攻撃に悪用される可能性を極力低減した形で無償または安価に提供したり、ベンチャーなどの企業における製造物責任の範囲を限定し、過重な責任負担が開発や運用の足かせとなるのを回避するなど、開発・運用支援の充実強化を図るとともに、そのような政府系研究機関と企業、大学による産学官連携を強化し、技術の融合による高付加価値化や市場からのフィードバックの反映などを通じて研究開発のより一層の効率性向上を図り、新たな需要を付加していくことが必要である。

出願人属性別の出願件数比率についてみると、日本国籍の出願人は、米国籍や欧州国籍の出願人に比べて、共同出願の出願件数の割合が低い。セキュリティの高付加価値化に向けて、産学官連携の重要性に対する意識を高めるとともに、開発支援資金の充実や開発技術・製品の民間移転の積極的な展開を図るなど、国産のセキュリティ技術・製品の開発を促進するための産学官連携の環境整備を推進していくことが重要である。

図 6-13
出願人国籍別－出願人属性別出願件数比率
（上左図は日本国籍の出願人、上右図は米国籍の出願人、下図は欧州国籍の出願人）



さらに、海外では、侵入検知やウイルス・マルウェア検知において、企業等が検知精度の向上のため、通信トラフィックなどの実データを収集し分析している。一方、日本においては、電気通信事業法第４条１項の通信の秘密の規定や、防衛など国家安全保障分野の守秘の規定により、海外の企業等と同様の行為を行うことができないのが実情である。このような制約を変えていくことには困難を伴うが、何らかの条件でもって、適切な形で規制緩和されれば、当該技術分野の技術競争力は好転する可能性がある。

他方、後者の仕組みについては、国家の研究開発プロジェクトや政府調達が果たすべき意義・役割が大きい。国家の研究開発プロジェクトにおいては、欧州の HORIZON2020 のようなスキームを参考にしつつ、応募の際に、技術力・開発力を持つステークホルダーと市場を持つステークホルダーのマッチングによる共同提案を提案の要件にし、開発された技術等を市場に適用しやすくする等の検討が必要である。また、政府調達においては、国家の研究開発プロジェクト等で開発された国産技術等を、政府機関や地方公共団体の情報システムの調達仕様・要件として盛り込むこと等の工夫により、導入の経済性はきわめて良好になると考えられる。

（提言２）情報セキュリティ分野の国産技術・製品の採用・実装に対する利用者側の意識を啓発・変革すべき

情報セキュリティ分野の技術・製品の利用者側において、国家安全保障や国内の重要情報保全の強化のために国産技術・製品を採用・実装することが重要であるという意識を持つとともに、それによって国産技術・製品の権益を保護すべきである。

我が国の国家安全保障や国内の重要情報保全の強化に向けて求められるセキュリティ分野の信頼できる国産技術・製品や信頼できる調達環境で生産される国産技術・製品については、企業のみの技術開発・研究開発や対応だけで全てを充足することには自ずと限界があることから、政府調達での採用やスペアとしての利用等による市場づくりや、技術導入を支援する認証制度の確立等を含め、オールジャパンでの国家プロジェクトとして、実用化や利用促進を政府が主導していくことが重要である。

なかでも特に重要な要素としては、海外と比べて、日本の技術競争力が劣っている侵入検知、ウイルス・マルウェア検知、ログ解析、リバースエンジニアリングといった領域での国産技術・製品の実用化を強化していくことと、暗号技術に関して、国産技術・製品の利用を促進し、これまで長年にわたり培ってきた企業の研究開発体制を維持することが挙げられる。暗号には、暗号化されたデータを元のデータに復号する復号が付き物であるため、これまで使用していたグローバルスタンダードの暗号を国産の暗号に切り替えることは簡単なことではない。国産の暗号で暗号化したデータを海外に送信したとき、海外でどうやって復号するのかという問題が生じる。このため、企業においては、暗号アルゴリズム領域ではなく、暗号を使ったアプリケーション領域でビジネスをせざるを得ない状況であり、暗号自体のビジネス展開が制約を受ける中で、昨今、投資対効果がより一層求められるようになり、研究開発体制を維持するのが非常に厳しくなってきている。（大手通信キャリアへのヒアリング結果より）企業の研究開発体制を維持していくにあたっては、政府調達での採用に加え、国家間の情報交換、通信の入口にある Internet Explorer のプロキシサーバのところで暗号アルゴリズムを、グローバル標準の暗号から国産の暗号に変換する仕組みを構築するなど、利用を促進する方法により、国産暗号の権益を保護していくことが重要である。

（提言３）IoT を活用する社会や産業に対応できるセキュリティ人材を育成・確保すべき

来たるべき IoT を活用する社会や産業において、日本が競争優位性を確立できるように、制御系システムや組込みソフトウェアの領域のセキュリティに対する知識や経験を持つセキュリティ人材の育成・確保や、制御系システム等のセキュリティに対する重要インフラや自動車等の関連企業、情報セキュリティ技術に携わる企業等の双方の理解の溝を埋める取組みを通じて、IoT を活用した制御系システム等において求められる情報セキュリティ分野の技

術・製品に関する技術開発、研究開発を、これまで以上に強力に推進していくべきである。

IoT を活用する社会や産業において求められるセキュリティ技術・製品・ツールを開発するうえで課題となるのが、セキュリティ人材の育成・確保である。

独立行政法人情報処理推進機構の「情報セキュリティ人材の育成に関する基礎調査」によると、日本においては、情報セキュリティに関する脅威・リスクが多様化・高度化する中で、これに対応したセキュリティ人材は約 2 万 2 千人不足し、約 14 万人あまりの人材に対しては、更に何らかの教育やトレーニングを行うことが必要になるなど、セキュリティ人材の育成・確保の必要性が指摘されている。取り分け、IoT に対応した制御系システムや組込みソフトウェアの領域のセキュリティは、これまでの一般 PC や企業等の事務処理系システムの領域のセキュリティとは異なり、メッセージの暗号化を 1 つとっても、活用可能なデバイスのリソースや通信の応答性に対する制約が厳しいとされる。（大手自動車メーカーへのヒアリング結果より）それにもかかわらず、セキュリティ人材の多くが、制御系システムや組込みソフトウェアの領域のセキュリティに対する知識や経験が必ずしも十分とは言えない状況である。また、株式会社富士キメラ総研の「2014 ネットワークセキュリティビジネス調査総覧」によると、日本のセキュリティ製品とセキュリティサービスを含めたセキュリティ市場の規模は約 4 千億円と言われており、一般 PC や企業等の事務処理系システム向けのセキュリティ対策のみで一定規模の市場が形成されていることも、制御系システムや組込みソフトウェアの領域へのセキュリティ人材の流動の足かせとなっている。セキュリティベンダーにおいても、足元のセキュリティ人材リソースの需給が逼迫する中で、目先の収益を最大化するために、マーケットサイズのパワーバランスという現実を直視して、一般 PC や企業等の事務処理系システム向けのセキュリティ対策の市場にセキュリティ人材を配置せざるを得ない状況にある。

中国では、政府が自国内のセキュリティ産業の振興を主導し、中国銀行業監督監理委員会が金融機関に対して、銀行の IT ガバナンスの強化や年間 IT 投資の 5%以上をセキュリティ関連投資に振り向けるよう通達（CBRC 通達 317 号）を出している。このような政府の関与の良し悪しについては、議論が分かれるところであるが、制御系システムや組込みソフトウェアの領域でのセキュリティ人材の育成・確保の成功を決定する大きな要因は、制御系システムや組込みソフトウェアの領域をどれだけ収益化できるか、そしてその際、セキュリティ対策にどれだけの費用を充当することができるかにかかっていると考えられる。

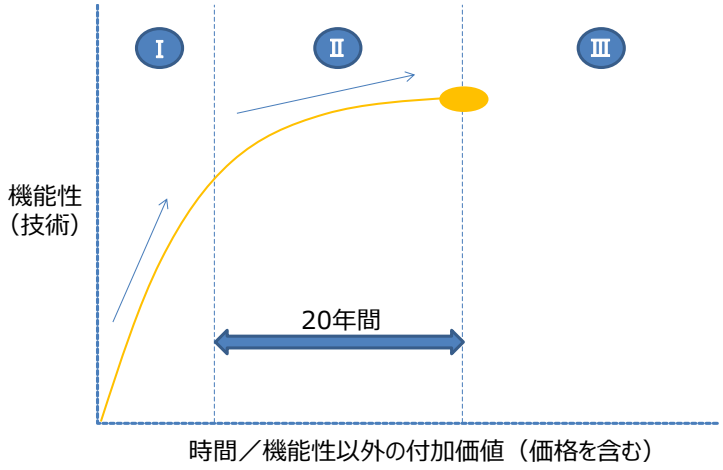
また、制御系システム等のセキュリティに対する、重要インフラや自動車等の関連企業、情報セキュリティ技術に携わる企業等の双方の理解の溝を埋めることも、制御系システムや組込みソフトウェアの領域でのセキュリティ人材の育成・確保を進めていくうえで重要である。双方が一堂に会して、IoT を活用した制御系システムや各種機器の組込みソフトウェア等に求められるセキュリティに関して議論できるような場を十分確保していくことが、制御系システム等のセキュリティに関する将来の技術開発をリードし、将来の市場を獲得していくうえで重要になるものと考えられる。

（提言４）IoT を活用した制御系システム等のセキュリティ分野における知財戦略を見直すべきである

IoT を活用した制御系システム等のセキュリティ分野に精通した知財支援人材の育成・確保や、日本のプレイヤーが開発した当該分野の技術・製品の海外輸出の加速によるデファクトスタンダードの獲得など、知的財産が果たすべき効用を活かしつつ、日本の競争優位性を確立すべきである。

グローバル市場で求められる制御系システムや組込みソフトウェアのセキュリティに関しては、グローバル知財戦略がきわめて重要である。弁護士法人内田・鮫島法律事務所の弁護士である鮫島正洋氏が東京工業大学で行った技術経営の講義の資料（平成 26 年度 R&D 戦略と知的財産戦略「特許から考える勝つための研究開発」）によると、ビジネスモデルの考え方と知財権の考え方より、以下のように事業のステージが定義されている。

図 6-14
事業のステージごとのビジネスモデルと知財権の考え方



ステージ Ⅰ ：必須特許出願可能ステージ ⇒ 創生期、発展期
知財戦略を徹底強化し、機能アップによる差別化、市場拡大・シェアを確保

ステージ Ⅱ ：必須特許満了までのステージ ⇒ 成熟期
コモディティ化を阻止、遅延し、投資回収・利益確保・知的財産権による権利行使

ステージ Ⅲ ：コモディティ化後 ⇒ 衰退期
別要因で競争

自動車や重要インフラのセキュリティの事業ステージは、今まさに創生期・発展期（ステージⅠ）にあたるものと考えられ、当該ステージにおいては、技術開発→必須特許取得という知財戦略の基本を励行し、市場が成長し、後発参入が始まるステージⅡに備えることが重要である。ステージⅠで先進的な技術を開発し、これを特許化した者が市場の成熟期（投資回収期）であるステージⅡで業界をコントロールでき、利益率の高い事業を遂行

できるようになると考えられる。

このような観点から、政府と企業、大学が一枚岩になり、半導体チップやHSM（Hardware Security Module）のセキュリティや、システム面のリソースや応答性の制約が大きい点や、制御機構の可用性やフェールセーフ化が重視される点など制御系システムにおける特性を踏まえた新しいセキュリティ技術、暗号技術分野での日本の強みを活かせる新しい暗号技術等に関わる必須特許を取得するための技術開発・研究開発の強化を強力に推進することが重要である。

これらに加えて、当該セキュリティ分野に精通した知財支援人材、または、グローバル知財戦略を遂行できる知財人材の育成・確保など、権利範囲の最大化や海外における適切な権利化等を実現できる特許の取得体制の強化や、日本が開発した技術を海外に売り込み、業界・市場のデファクトスタンダードを獲得するためのパッケージソリューション化やプロモーション活動についても強力に推進することが重要である。

さらに、非競争領域の情報セキュリティ技術については、市場の更なる拡大に貢献するとともに、一般のPC等のセキュリティの世界と同様、長期にわたって攻撃と対策等に関するデータを幅広く収集・分析し、新しい情報セキュリティ技術・製品の開発に繋がる技術力や知見・ノウハウを継続的に蓄積する仕組みを構築するなどの方法や、必須特許の特許切れや次なるビジネスの創出に備えることにより、競争優位性を高めていくことが重要である。