資料４

情報セキュリティ研究開発戦略（改定版）（仮）
【パブリックコメント案】

２０１４年　月　日

技術戦略専門委員会

目次

１　はじめに

我が国の情報セキュリティ研究開発は、これまで以下のように進めてきた。

・情報セキュリティ政策会議において、２０１１年７月に「情報セキュリティ研究開発戦略」を決定した。そこでは、２０１１年度から２０１５年度までの５年間及び中長期的な研究開発の課題及び１２の重点分野について検討し、取りまとめを行った。
・また、２０１２年６月には「情報セキュリティ研究開発ロードマップ」を技術戦略専門委員会において策定し、「情報セキュリティ研究開発戦略」の１２の重要分野をさらに３３の項目に分け、それぞれの要素課題についての達成目標等について具体的なまとめを行った。
・政府等の研究開発としては、これらの計画も踏まえ、各種情報セキュリティ研究開発施策を推進してきた。

しかし、ネットワークへ接続するシステムや機器が従来より大幅に拡大していっている中で、サイバー攻撃が複雑・巧妙化するなど、情報セキュリティを取り巻く環境が著しく変化しており、より柔軟かつ実践的な取組が求められるようになってきた。

こうした中、情報セキュリティ政策会議は、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、新たな情報セキュリティ戦略として、世界を率先する強靭で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」を実現することを基本的な方針とする「サイバーセキュリティ戦略」を２０１３年６月１０日に決定した。この中で研究開発については我が国のサイバー防御能力の向上、経済成長につながる新産業創出、国際競争力の向上のために重要なものと位置付けられている。

また、２０２０年には東京でオリンピック・パラリンピックが開催され、情報セキュリティを含め我が国の安全安心な技術に世界中から注目が集まることから、より一層我が国の技術力、国際競争力を強化していくことが必要である。

本「情報セキュリティ研究開発戦略（改定版）（仮）」（以下、「研究開発戦略」という。）はこのような状況を踏まえ、「サイバーセキュリティ戦略」に基づき、国民・企業・国家の情報や権利を守り、ＩＴ（情報通信技術）を安全に安心して便利に利活用できる社会を実現するべく、我が国における情報セキュリティ研究開発を、従来よりも更に実践的・有効的に実施していくために、今後３年程度を見据えた基本的方針を示したものである。

今後、本研究開発戦略に基づき、政府や公的研究機関等での研究開発が推進されるとともに、大学や企業等における情報セキュリティ研究開発においても、産学官で互いに連携して推進され、我が国の情報セキュリティ研究開発能力を高めていくことを目指していく。

２　これまでの情報セキュリティ研究開発

（１）情報セキュリティ研究開発の進捗状況

情報セキュリティ研究開発は、「情報セキュリティ研究開発戦略」（２０１１年７月策定版）では、東日本大震災も踏まえた、「能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術の研究開発を促進する」という考え方の下、２０１５年度までの目標実現に向けた研究開発を推進してきた。

そこで示した１２の重要分野の進捗状況についてみると、「大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合」「情報理論的安全性を備えた暗号技術」といった研究テーマについてはおおむね順調に進んでいる一方、「システムのセキュリティ設定を上位から下位まで自動保証する技術」「障害に対して自動回復可能なネットワーク構築技術」といったテーマについては、その後のサイバー攻撃の対策への重点化の変化等により、公的研究機関等の情報セキュリティ関連部門の研究では十分な進捗が見られていない状況である。

また、「サイバーセキュリティ戦略」において記載されているサイバー攻撃の検知、制御システムのセキュリティなど、現行の研究開発戦略の重点分野の領域以外で取り組みが必要となっている研究も新たに多数出てきている。

表１　情報セキュリティ研究開発戦略（２０１１年７月策定版）における重要分野

情報通信システム全体のニュー・ディペンダビリティの確保	
①	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術
②	システムのセキュリティ設定を上位から下位まで自動保証する技術
③	障害に対する自動回復可能なコンピュータネットワーク構築技術
④	生体情報をコンピュータで管理するための ID 管理と生体情報を統合するシステム設計構築技術
攻撃者の行動分析に基づくゼロデイ・ディフェンス	
⑤	攻撃者の行動分析等による予防基盤技術
⑥	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合

個人情報等の柔軟管理の実現	
⑦	個人情報等の利活用を促進する自己情報の統制技術
⑧	フォレンジック等を支援するためのデータ管理・追跡技術
⑨	IT リスクに関する理論から実務までの体系化
研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	情報セキュリティ研究の基盤体系化
⑪	セキュリティ部品が正しく実装されていることを保証する製品評価認証技術
⑫	情報理論的安全性を備えた暗号技術

（２）情報セキュリティに係る予算の動向

「情報セキュリティ研究開発戦略」（２０１１年７月策定版）では２０１１年度から２０１５年度までの５年間に重点的に取り組むべき情報セキュリティ研究開発分野を特定し、研究開発予算の充実を掲げている。

しかし、政府の情報セキュリティ研究開発予算は２００７年度から２０１４年度までを比較すると、補正予算等により大幅に研究開発予算が増加している年度もあるものの、当初予算は全体としては減少傾向となっている（図１）。

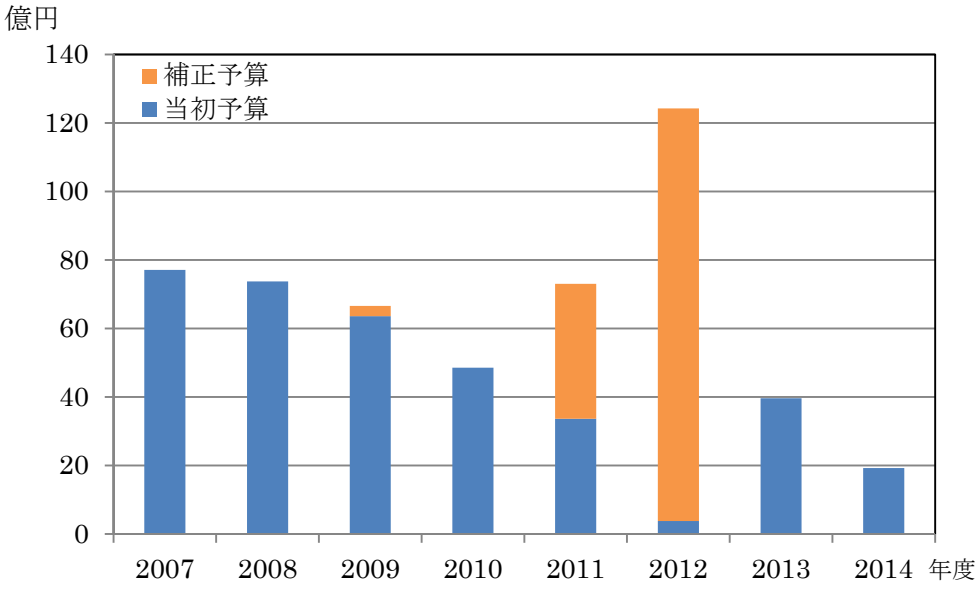


図１：日本政府の情報セキュリティ研究開発予算の推移[1]

[1] ２０１０年度以前は、情報セキュリティ研究開発戦略（２０１１年７月策定版）の値を使用。２０１１年度以降は、内閣官房情報セキュリティセンターに登録された情報セキュリティ予算から、研究開発に該当するものを事務局で計上。各年度の値に独立行政法人の運営費交付金の内数等は含まず。

他国の例として、米国の情報セキュリティ研究予算をみると２００７年度から２０１４年度までで大幅に増加している（図２）。そのため、情報セキュリティ研究開発予算の GDP 比率（米国／日本）[2]は、２００７年度においては約１．２倍であったものが２０１３年度においては約４．７倍、２０１４年度では約１２倍と拡大している。

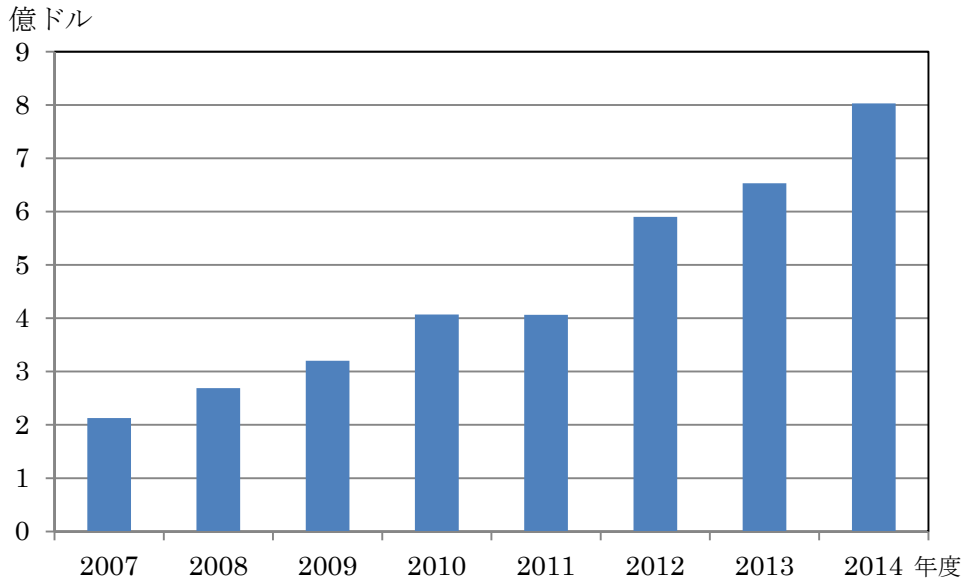


図２：米国政府（NITRD CSIA）の情報セキュリティ研究開発予算の推移
（２０１３年度、２０１４年度は予算要求額）

[2] 研究開発予算の GDP 比率（米国／日本）は、（米国の情報セキュリティ研究開発予算）÷（米国の GDP）と（日本の情報セキュリティ研究開発予算）÷（日本の GDP）との比により算出。また、日米の GDP は IMF - World Economic Outlook Databases より引用。

他方、我が国における研究開発以外も含む政府全体の情報セキュリティに係る予算は増加傾向にある（図３）。２０１４年度予算では、大規模サイバー攻撃事態に対処するための機能の強化、サイバー攻撃複合防御モデル・実践演習、各国のサイバー攻撃対応連絡調整窓口ＣＳＩＲＴ(インシデント対応チーム)の間での情報共有や共同対処を行う枠組み構築等のサイバーセキュリティ経済基盤構築事業、サイバー情報収集装置の整備等、サイバーセキュリティの被害が深刻になる中、より実践的な施策を推進するための予算となっている。全体としては、サイバー攻撃への対策予算の高まりが見られる。

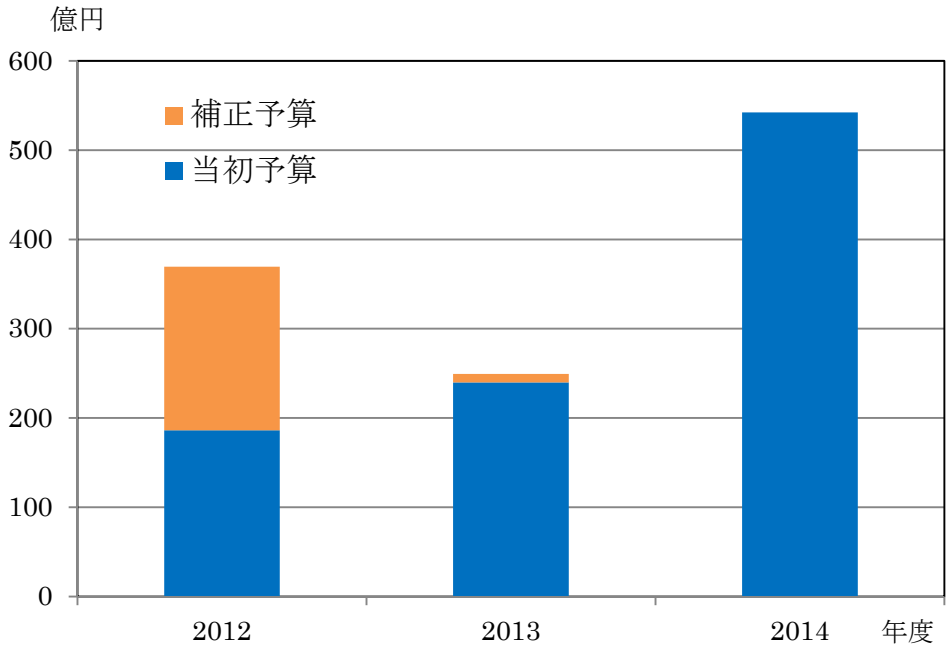


図３：政府の情報セキュリティに係る予算
（内閣官房情報セキュリティセンターで集計）

（３）「サイバーセキュリティ戦略」等を踏まえた、「研究開発戦略」の見直し

ＩＴ（情報通信技術）は、個人や家庭等の私的な空間から社会インフラ等の公的な空間、機器やデバイスの内部まで隅々に行き渡り、経済・生活基盤を支え国家の成長を牽引する存在となっている。一方で、これらのシステム、ネットワーク等に障害が発生すれば社会に深刻な影響を及ぼすこととなる。サイバー空間を取り巻くリスクは拡大し続けており、これまで以上に情報セキュリティ対策が重要になっている。

このような近年の情報セキュティを取り巻く環境変化も踏まえ、「サイバーセキュリティ戦略」においては、海外の技術、サービスや製品への依存度が高いことから、研究開発等を通じて国際競争力を強化することが必要であること、変化の激しい情勢に適切に対応できる、創意と工夫に満ちた情報セキュリティ技術を生み出していくことが重要であること、研究開発等で得られた知見により、経済成長につながる新産業創出が期待されることについて指摘した上で、具体的な方針として、①「サイバー攻撃の検知・防御能力の向上」、②「制御システム、ＩＣチップなど社会システム等を保護するためのセキュリティ技術の確立」、③「ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発」、及び④「国際標準化や評価・認証を含んだ制度整備等」が示されたところである。

以上のような課題を解決すべく、大学や公的研究機関等に期待される役割等も含め、従来よりも更に実践的で有効に成果が用いられる研究開発となるよう、研究開発戦略の見直しを行う。

３　研究開発戦略の見直しにあたっての課題

サイバーセキュリティ戦略から導かれる３点の基本的方針及び国際連携の観点を踏まえ、研究開発の進め方についての課題を後述の（１）①～⑤の５つの観点で整理する。（なお、今後の情報セキュリティ研究開発取組方針について４章で記載する）

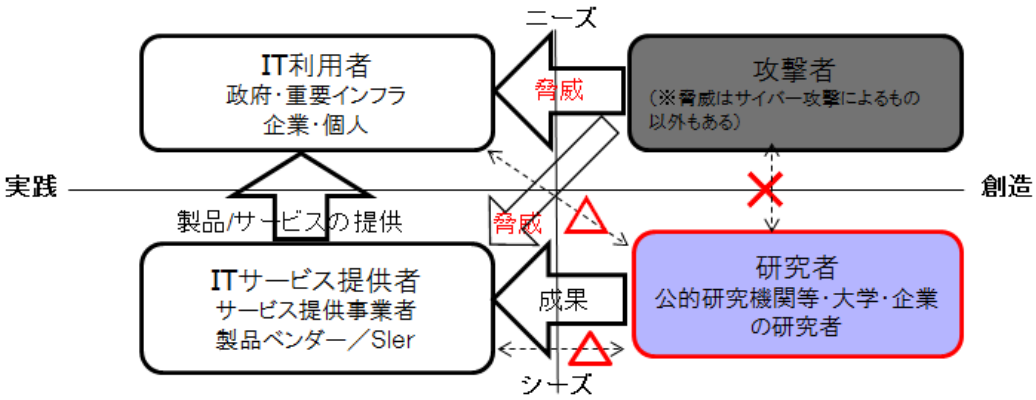
また、研究開発の範囲・リソース等について考慮する必要があるため、研究開発・効果を高めるにあたっての課題について（２）①～③に示す３つの観点で整理する。（なお、研究開発・効果を高めるための施策については５章で記載する）

（１）研究開発の推進方針における課題

① サイバー攻撃の検知・防御能力の向上における課題

サイバー攻撃が高度化・複雑化している中で、より実践的な研究開発の推進が求められていると考えられることから、研究開発に当たっては、現実にどのような脅威があり、具体的なニーズが何であるかということを適時適切に把握して取り組むための環境等の整備の必要性がある。

サイバーセキュリティ関連等の研究者と脅威やニーズの情報流通の関係を検討すると以下のような状況にあると考えられる（図４）。



×：情報共有・理解がほとんどないと思われる

△：情報共有・理解が十分でないと思われる

図４：　研究者と脅威やニーズの情報流通の関係

攻撃者による手法などは日々高度化・巧妙化し、ＩＴ利用者においては、脅威や発生している事象に気付くのが困難となってきている。また、このような

状況の下で、ＩＴサービス提供者においても、適切な製品・サービスの提供が難しくなりつつあると考えられる。

そして、情報セキュリティ対策の実践側（ＩＴ利用者、ＩＴサービス提供者）において、サイバー攻撃等の状況やニーズが不明確であると、研究者は、現実の脅威や将来高い確度で発生しうる脅威などを予測などして、適切な課題・境界条件を設定して、研究を行うことが難しくなっていくと考えられる。情報セキュリティに係る研究開発活動をより一層活性化するためには、研究開発に必要な情報等（脅威やニーズに関するものなど）が十分に循環しない状況であることや、我が国においては攻撃者視点の情報を研究者において把握することが難しいことなど、研究開発をより実践的なものとしていくにあたっての課題（具体的な事象などの脅威に関する情報やユーザ等のニーズに関する情報の共有の必要性への対応等）を解決することが重要である。

その際、従来よりも実践的で有効に成果が用いられるような研究開発の推進方針の検討にあたっては、現在の情報セキュリティ関連の研究者のリソースに限りがあり、異なる分野間のやり取りが十分でないという状況を踏まえて考える必要があるため、情報集約や情報共有の取組が課題となっている。

② 社会システム等を防護するためのセキュリティ技術の強化における課題

現在あらゆるところでＩＴが利用される中で、社会インフラを構成する重要インフラの制御システムなどにおけるセキュリティ対策は、国民の安全安心な生活や、国家の安全保障・危機管理上の課題となっている。例えば、Ｓｔｕｘｎｅｔ[3] にみられるように基幹的なインフラの制御系システムに対して、ＵＳＢメモリを媒介してコンピュータウイルスに感染させ、インフラにおける機器を稼働不能とするような攻撃も現実のリスクとなってきている。

③ 産業活性化につながる新サービス等におけるセキュリティ研究開発の課題

企業等が情報セキュリティに係る研究開発に積極的に投資するか否かは、将来の競争力につながる事業化が見込めるかどうかが重要なファクターとなる。情報セキュリティの確保はあらゆる分野で必要であるが、特に今後ＩＴの利活用により発展が期待される分野（健康・医療分野、社会インフラ、自動車のネットワーク接続等）において上流工程から情報セキュリティを確保することが重要となってくる。また、スマート化が進展する中、一般消費者が今まで以上

[3] 「Stuxnet（スタックスネット）」は、インターネットから隔離されたスタンドアローンの産業用制御システムにおいても感染し実害を生じるウイルス。2010 年 11 月 ウラン濃縮施設へのサイバー攻撃等で使用されたとされる。

にサイバー攻撃にさらされることになるが、そうした脅威から守るための製品・サービス開発は、産業の活性化にも期待される。

④ 情報セキュリティのコア技術の保持

暗号などの技術やその評価能力は、機密情報の保護などの観点から、重要な技術である。しかしながら、直接的にビジネスにつながりにくいなどの理由から、民間事業者等においては、研究開発体制の維持が難しくなっている傾向がある。このような背景も踏まえ、我が国として技術力の保持が必要と考えられる事項について、公的研究機関等にて研究体制を維持・強化していく必要がある。

また、ＩＴサービス提供者については、ＩＴ利用者のニーズを把握できたとしても、次のような課題が残る。現在、あらゆる産業分野で情報システムが利用されるが、システムのＯＳなど重要な製品が海外製品となり、国内技術の空洞化が生じている状況のもとでは、根本的な解決策を検討できない、対策を措置できないといった課題を抱えるということになる。したがって、重要な技術・製品等については、我が国としても必要な技術力を獲得・保持するべきであることとともに、情報セキュリティが国境を越えるボーダレスな問題であることを踏まえると、これらの技術力はグローバルに通用するものであるとともに産業競争力のあるものとする必要がある。

⑤ 国際連携による研究開発の強化等

高度なサイバー攻撃から我が国、自組織を守るためには、攻撃者の能力を超えて対応できることが必要であることから、情報セキュリティの研究開発においてもグローバル水準を上回るものであるべきである。そのためには海外の先進的な研究機関等との国際連携や、先進的な研究機関と人材交流、優秀な研究者・技術者の確保などが課題となる。

（２）研究開発の効果・成果を高めるにあたっての課題

情報セキュリティにおけるリスクが甚大化、拡散、グローバル化している一方で、我が国では、公的研究機関における研究体制等のリソースが限られていることから、従来よりも更に研究開発の効果・成果を高めていく取組が求められている。

研究開発の効果・成果を高めるための課題としては、前述の脅威やニーズ情報の研究者への流通以外に、以下のようなものが考えられる。

① 情報セキュリティ技術は実用化されることが重要であるが、現状では研究成果が必ずしも社会還元に結びついていないとの指摘がある。また、情報セキュリティの研究成果を活用したベンチャー企業の育成等の産業活性化に結び付いていないとの指摘がある。

② 情報セキュリティの脅威や対策、研究開発テーマの範囲は多岐にわたり、ＩＴや情報セキュリティ技術の変化も激しいが、そのために必要な研究開発リソースの確保と柔軟性確保が十分とはいえない。

③ ＩＴ利用者及び攻撃者側の問題、動機、同行を把握・理解し、適切な対応策を立てられるようにするには、技術的な観点からの検討だけではなく、海外の情報収集・分析や、社会科学（国際情勢、安全保障、危機管理、経済学、経営学、心理学、法学等）など他分野と融合した取組が必要であるが、我が国ではこうした取組が十分でない。

4　今後の情報セキュリティ研究開発取組方針

３章で示した課題の解決につながるような研究開発を進めるため、研究開発の取組方針や、今後取り組むべき施策例を、以下に示す５つの観点で整理する。

（１）サイバー攻撃の検知・防御能力の向上

高度なサイバー攻撃を検知し対処できるようにするためには、継続した研究開発や技術開発によるサイバー攻撃の検知・防御能力の向上が重要である。その際に、最新のサイバー攻撃の実態や動向といった攻撃者側の視点や、組織内におけるネットワークのあり方といったネットワーク利用者側の視点など多角的な研究開発を行うことで、社会ニーズにも合致した大きな成果が期待できる。

情報セキュリティの研究開発分野には、コンピュータ・ネットワーク防御（ＣＮＤ：Computer Network Defense）や情報保証（ＩＡ：Information Assurance）、情報セキュリティマネジメント、暗号等の基礎分野など様々な専門領域があるが、これらの研究開発の充実に役立つ情報やデータが研究者等において十分に得られていない場合もあり、このことが効果的な研究開発の実現を妨げている一因と考えられる。そのため、最新の攻撃の動向や現状の課題など、研究開発に必要となる情報やデータが共有されることで、研究開発の成果が最大化され、その成果をもとに最新のサイバー攻撃が検知され、情報が蓄積・共有されるという研究開発の好循環を実現することが重要である。

したがって、多角的な研究開発を実現し、我が国のサイバー攻撃防御能力を一層向上させるためには、研究開発における実際のサイバー攻撃情報等の重要性に鑑み、研究開発に資する現実の情報やデータ、限られたリソースを分散させることなく、集約して進めるとともに、政府全体としての情報共有及び、そのための組織等の連携強化を可能な範囲で推進していくことが必要である。また、より実践的な研究開発のために、可能な範囲・方法・条件で研究者等への情報提供等についても検討していくことが必要である。

さらに、コンピュータウイルスやマルウェアの解析をする際には、リバースエンジニアリングによる解析が一つの有効な手段と考えられるが、国内企業では著作権法などに抵触しないかといった懸念が持たれており、フェアユースな情報セキュリティ目的のリバースエンジニアリングに対する適法性の解釈の明確化や周知が求められている。

［推進すべき施策例］

- 我が国が保有するサイバー攻撃情報やデータは、政府機関情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）、ＪＰＣＥＲＴコーディネーションセンター、サイバー情報共有イニシアティブ（Ｊ－ＣＳＩＰ）、一般財団法人日本データ通信協会テレコム・アイザック推進会議、サイバーインテリジェンス情報共有ネットワーク、サイバーディフェンス連携協議会等の複数の組織・システムにおいて収集されている。しかし、これらで収集した情報やデータの共有先は各グループ内に限られている傾向がある。サイバー攻撃への対応能力や攻撃者に関する把握能力を高めるため、関係者と調整しつつ、更なるサイバー攻撃情報の共有を推進する。
- より実践的な情報セキュリティ研究開発のために、標的型攻撃で用いられる検体や関連データの利用が、研究者等から求められていることを踏まえ、秘密保持契約などにより必要な措置を施したうえで、より実践的な研究開発実施のために可能な範囲・方法・条件で政府が保有する検体等の攻撃情報やデータを研究者等へ提供、または内閣官房情報セキュリティセンターの特定グループへの一定期間の研究者受け入れ（研究者が実務経験を積める場としての目的も兼ねる）等を検討する。
- 巧妙化・複雑化する新たなサイバー攻撃に対応するためには、最新のサイバー攻撃の情報をもとに、有効な対策を立案し、実施する必要がある。このため、新たな攻撃を検知し、解析するための環境整備を推進する。
- 利用者のネットワーク環境の特性や行動特性、通信頻度などを解析し、それらの解析結果に基づいた利用者ごとのリスク分析や効率的なサイバー攻撃検知を行うとともに、攻撃発生時に自動的にネットワーク構成を変更するといった有効な防御方式に関する研究開発を実施する。
- 個人の利用者において、マルウェアに感染したユーザを検知し、マルウェアの除去を促すとともに、マルウェアを配布するサイトやフィッシングサイト等の悪性サイトの情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする利用者に対して注意喚起を実施する取組について、国際的な展開を視野に入れつつ推進する。
- サイバー攻撃可視化技術やサイバー演習環境構築技術の研究開発を推進する。
- フェアユースとしての、情報セキュリティ目的のリバースエンジニアリングの適法性を明確化するための措置を国として速やかに講じていく。

（２）社会システム等を防護するためのセキュリティ技術の強化

社会インフラを構成する重要インフラの制御システムなどにおけるセキュリティ対策は、国民の安全安心な生活や、国家の安全保障・危機管理上の課題となっている。このため、制御システム等、社会インフラ等を構成する要素に関する研究開発が必要となってきているが、社会インフラを構成するシステムは多種多様で、対象が広範囲であることから、重点的に進めていく分野を特定しつつ研究開発を進めていく。

また、社会システム等を構成する制御システム等のセキュリティ技術の研究開発にあたっては成果の早期実用化やインフラ技術の国際展開などが重要であることに鑑み、国際標準化・国際的な適合性評価制度につなげるよう推進していく。

［推進すべき施策例］

- 経済産業省では、２０１３年４月から稼働している制御システムセキュリティセンター（ＣＳＳＣ）において、制御システムのセキュリティ向上のための技術や制御機器の評価・認証をするため、研究開発、国際標準化活動、評価認証基盤整備等が実施されている。今後、ＣＳＳＣにおいて、重要インフラ等に利用される制御システムに関する研究開発の推進と併せて、制御システムセキュリティに係る国際標準化の推進とそれをベースとした国際的な相互認証制度の確立を行う。
- さらに、ＣＳＳＣに構築したテストベット施設を中核として、制御システムのセキュリティ検証方法及び第三者による評価・認証方法に関する研究開発に取り組み技術的基盤を確立していく。
- また、セキュリティに係る半導体チップの模造や改竄、情報通信ネットワークにおける機密情報の漏洩や個人データの盗取等のセキュリティ事案の解決に向けた、セキュリティチップ等の最先端暗号技術の導入と真正性を保証する半導体デバイス製造・流通の確立のための研究開発を実施する。
- 自動車と携帯端末等の機器との接続が拡大するにあたって、情報セキュリティ上の諸問題（認証等）について調査し、セキュリティ技術の開発・国際標準化への対応について検討する。

（３）産業活性化につながる新サービス等におけるセキュリティ研究開発

現在、情報通信技術は、個人や家庭等の私的空間から社会インフラ等の公的空間まで利用されているが、産業活性化・国際競争力の強化の観点から、ＩＴ

の利活用により更なる発展が期待される分野において、企画・設計段階などの上流工程からセキュリティ品質を組み込むことが必要である。これにより、日本ブランド品質のひとつとしてセキュリティを位置付けて、日本発のグローバルＩＴ製品・サービスの実現を目指していく。

今後ＩＴの利活用により発展が期待される分野（「世界最先端ＩＴ国家創造宣言」）のうち、情報セキュリティ技術が求められる分野として、例えば以下のような分野が考えられる。

- 医療健康分野（情報連携ネットワークの全国への普及・展開を行う際の、個人情報を守るための、セキュリティ品質確保等）
- スマートな次世代インフラ分野（災害関連情報の収集・提供等のシステムについて、大規模災害時の安定的稼働や個人情報等を守るためのセキュリティ品質確保等）
- ビッグデータの利活用分野（プライバシー情報等のセキュリティ保護）

［推進すべき施策例］

- ＩＴの利活用により更なる発展が期待される分野において、企画・設計段階などの上流工程からセキュリティ品質を組み込むことを目指す。そのため、例えば政府が推進する研究開発プロジェクト、社会システムの基本設計プロジェクトのうち、新たに情報通信ネットワーク接続を伴うシステム等（例：自動車のネットワーク接続や、医療情報など、人の生命や財産・権利に係るようなシステム）の公募要領や選定基準、プロジェクトマネージメントなどにおいて、研究・開発・企画の段階から情報セキュリティを組み込むよう方針を提示していく。

（４）情報セキュリティのコア技術の保持

変化の激しい情勢に適切に対応し、日々高度化・巧妙化するサイバー攻撃等に前もって予測して対応（プロアクティブに対応）していくためには、攻撃や防御のための技術の原理、システム等の仕組みなどを自ら考え、開発していくことができる必要がある。そのためには、まずは我が国において発生している事象のデータを解析でき、さらにはグローバルに発生している事象を把握できることが重要である。このようなことを可能とするためには、欧米のグローバルなセキュリティ企業、ＩＴ企業での事例をみても、ＩＴ製品やサービスがグローバルに展開されることを視野に研究開発をすることが重要である。グローバル展開で得られたデータや情報が、コンピュータ・ネットワーク防御（ＣＮ

D）などに係るコア技術やシステム化技術を検討していくにあたり有効な基礎力となると考える。

また、暗号については、欧米をはじめ諸外国において電子政府等において用いるべきものを指定又は推奨されている。その中には、自国で開発された暗号などが含まれており、国際標準化なども進められている。我が国においても、同様に、国際標準化などされた我が国の暗号を含め、ＣＲＹＰＴＲＥＣでの評価を踏まえて電子政府推奨暗号リスト化されている。暗号は、国の機密情報の保護をはじめ、商用においても認証など様々な分野で基盤として用いられているが、危殆化する前により強固な暗号へ移行することが不可欠な特徴がある。

したがって、引き続き、暗号技術の動向を把握し、評価し、必要な開発能力を維持する必要がある。

ＩＴの普及と利活用が進み、国民の生活が豊かになる一方で、なりすましや情報改ざん等これらの情報を狙ったサイバー攻撃も発生している。これらの脅威への対抗技術として、通信相手の権限の有無を確認した上で通信を行う認証の仕組みがある。人の認証、モノの認証など、個別の認証システムが多数存在する中で、利用者やサービス提供者側の手間の増加や情報セキュリティの確保等の課題も存在しており、安全かつ利便性の高い認証が求められている。例えば、ＩＤ連携などによる便利な認証環境の構築や、ＩＴを活用した確実で、利便性の高い本人認証が可能となることが考えられる。また、様々なモノがネットワークで接続される中で、機器間通信（Ｍ２Ｍ）の活用が期待されるところ、モノの認証により情報セキュリティ上の機密性・完全性を確保することで、Ｍ２Ｍの普及展開が期待できる。このような社会インフラの基礎となる技術も我が国の社会の安全確保の観点から、我が国として基盤技術を保持することが重要である。

特に注意したい点は、研究開発においては、結果的には思い通りの成果が得られないことも多いが、近年、研究開発に対する成果を求める傾向が強くなっており、長期にわたる基礎研究やリスクの高い研究にチャレンジすることをためらう傾向があるとした指摘がある。今後、我が国として、基礎研究を含めより一層の研究開発レベルの向上を図っていくためにも、研究開発関係者がリスクにチャレンジする文化や、失敗しても再チャレンジし新しいイノベーションを起こしていく文化を醸成することが重要である。

［推進すべき施策例］

・ 基礎研究は、直ちにはビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障等の観点から国として維持することが不可欠な技術もある。この

ため、特に国として維持することが技術については、公的研究機関等や大学などをはじめ適切な研究機関等において、若手を含め研究者が活躍できる環境を維持していくべきである。具体的には、ＣＲＹＰＴＲＥＣの事務局などを担当する独立行政法人などを中心に、暗号研究の着実な推進が重要である。

- ＩＴ利用者に対する利便性向上とＩＴ利活用拡大を図るため、ＩＤ連携などの仕組みを戦略的に整備していくとともに、生体認証など、確実な本人認証を行える基礎的な技術の開発の能力を維持・発展させるべく関連プロジェクトを推進する。
- モノのインターネット（Internet of Things（IoT））の拡大に伴い、情報セキュリティ上の脅威の及ぶ範囲が拡大しつつある状況を踏まえ、機器間通信（Ｍ２Ｍ）の認証の情報セキュリティ技術の開発・実証を行うことで、Ｍ２Ｍの更なる普及・展開を図る。
- また、我が国の技術力を支えるのは、研究者や現場の技術者１人１人であり、大学や各研究機関においては、研究開発を通じて、我が国を支える研究者の育成に努めていくことが必要である。

（５）国際連携による研究開発の強化等

サイバー空間には国境がなく、サイバー攻撃も国を越えて行われることから、高度化・巧妙化するサイバー脅威に対処するための技術的な対応にあたっては、国際的に連携して、より高度な対策技術の開発が必要である。このため、サイバー攻撃等に的確に対応できる高度な対策技術の開発に向け、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効であり、国際連携による研究開発を積極的に行うことが求められる。

その際、国際連携のパートナーを選定するにあたっては、我が国やサイバー空間を脅かすおそれがないかどうかの観点から慎重に見極める必要がある。また、日本の研究者側の情報保全を高め、相手方の信頼を得ることが不可欠である。

サイバー空間のセキュリティを確保するためのシステムや機器などは広く国際的に取引されるようになってきているが、その相互運用性や求められるセキュリティ水準を確保するための技術的な標準の重要性が増している。このため、様々な国際標準化の取組が行われている中で、サイバーセキュリティ技術に関する国際標準の策定・普及や相互承認枠組作りを進めていくことが重要である。

［推進すべき施策例］

- サイバー攻撃、マルウェア等に関する情報を収集するネットワークを諸外国と連携して構築し、サイバー攻撃の予兆を検知し、迅速に対応することを可能とする技術の研究開発・実証実験を実施するプロジェクト PRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）を進めているが、２０１３年９月に行われた日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議の成果を踏まえ、ネットワークセキュリティ分野における技術協力プロジェクト（JASPER）を推進することにより、グローバルレベルでのサイバー攻撃の予兆の検知及び対応の迅速化に貢献する。
- ＣＳＳＣ（制御システムセキュリティセンター）を拠点として制御システムセキュリティの評価・認証技術を確立するとともに、ＣＳＳＣに参加する企業や団体を中心としてＣＳＳＣの活用による新たな国際標準の提案活動を行っていく。
- 研究開発力の強化や高度な技術開発のために、国際連携による研究開発を推進する。例えば、海外の先進的な情報セキュリティ研究機関への留学や、国内研究機関での海外からの優秀な人材の受け入れ、共同研究などの支援の充実を図る。

５　研究開発の効果・成果を高めるための方策等

これまでも述べたとおり、情報セキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であることを鑑みれば、前述の研究開発取組方針の各施策の実施などを行うにあたっては、研究成果の社会還元が十分に行われることや、社会的なニーズを把握できる仕組みが必要となる。また、研究開発を実施するに当たっては、必要なリソースの確保が必要となってくる。

このため、前述の研究開発取組方針の実施にあたり、以下のような研究開発の効果・成果を高めるための方策等を進める必要がある。

（１）研究成果の社会還元の推進

前述のとおり、情報セキュリティを巡る脅威やニーズといった研究開発に必要な情報等が十分に循環しない状況を改善し、攻撃情報やニーズの集約化を行うことにより、社会的なニーズに対応した研究開発の促進を行っていくことが重要である。この際に、研究の早い段階から、ＩＴ機器利用者や運用者と協働し、研究者以外の視点を取り入れることも求められる。また、ＩＴサービスの提供を行っている者と研究者との間での情報流通が現在十分でないことを鑑みると、研究を行っている者と実用化を担う者との間をつなぐ人材の配置、育成が必要である。

また、社会還元の仕組みについて、諸外国の事例を見ると、米国では、プレＲ＆Ｄ（研究開発前段階）、ポストＲ＆Ｄ（実用化前段階）などのプロセスを設け、プレＲ＆Ｄ（研究開発前段階）の中で、課題抽出やニーズの特定、技術の効果/実現可能性の検証などを実施している。欧州、韓国でも、研究成果の社会還元を促進するため、技術移転部門を活用し技術移転を行っている。

我が国でも社会還元に取り組んだり、公的研究機関等で社会還元部門があるが、こうした海外での取組を参考に研究開発成果を社会還元する取組を強化することが望ましいと考えられる。例えば、各研究機関の社会還元促進部門等を通じ、契約面や広報面の充実をはかりつつ、ニーズシーズのマッチングや、研究成果の社会還元の促進・研究開発成果を広く産業界に還元していくとともに、研究成果の社会還元の達成度合いの確認や分析を行い、その仕組みの改善を図っていくことが望まれる。

また、今後の我が国の産業活性化のためには、新規事業に挑戦するベンチャー企業等の活性化が重要であるが、そのための施策として、公的研究機関とベンチャー企業との共同研究や研究開発成果を活用したベンチャー企業の育成を進めるとともに、ベンチャー企業を指導・支援する専門家、メンター等をベ

ンチャー企業支援施策に取り込んで、経営・事業化等のノウハウを活用する方策を検討していくことが望まれる。

（２）必要な研究開発リソースの確保と柔軟性確保

情報セキュリティを巡るグローバルな競争を勝ち抜くためには、研究開発投資の確保、基礎力となるコア技術の保持などが必要である。そのためには、技術力を高めるため研究開発投資が求められるところであるが、我が国の情報セキュリティ研究開発予算は増加しているとは言えない状況である。

一方、米国、欧州、韓国では、情報セキュリティの研究開発予算は年々増加しており、政府が積極的に民間の研究開発を支援している。また、米国国防総省国防高等研究計画局（ＤＡＲＰＡ）では政府が積極的に政府調達を実施している。

また、我が国では、研究を実施するにあたり、研究開発予算のテーマ・実施内容が年度当初に確定されており、新たな課題が発生した際への緊急対応が困難となること、予算の費目等が限定されており使い勝手がよくないこと、執行の手続きが煩雑であるために、研究者が研究開発ではなく予算施行手続きや評価対応手続きに多くの時間を割かざるを得ないことなどが問題として指摘されている。研究資金や研究者を支援する体制の充実、年度途中からでも新たな脅威に対する研究活動が開始できるように、また、研究者がルールを遵守しつつ、研究に専念できるよう必要な予算をより柔軟に活用できるような制度の採用などが求められる。

情報セキュリティ研究開発においても基礎研究は重要であり、研究者が多様で独創的な研究開発に取り組めるよう、競争的研究資金制度等の研究開発資金について、運用面での整合性や使い勝手を改善するとともに、優れた研究に対して基礎から応用まで切れ目ないリソース供与を可能とするための府省・制度の枠を超えた制度の在り方、さらにピアレビューなどで適切な評価の在り方の検討が重要である。

これらの課題に対処するために、関係省庁等と連携しつつ、我が国における情報セキュリティ技術の研究開発に必要な予算を確保するよう努めるとともに、情報セキュリティ政策会議が司令塔となって、研究開発予算に係る課題の把握や情報セキュリティの研究開発体制の整備、研究開発のためのリソースの柔軟性確保に向けた取り組みを促進していく。

なお、情報セキュリティの研究開発が必要な技術領域・応用分野が拡大しており、これらをカバーできるような研究人材の育成、研究体制の確保も求められる。

（３）情報セキュリティ技術と社会科学、経営学など他分野との融合

情報セキュリティ上の脅威は、組織の運営・事業継続だけでなく、国家の安全保障や経済にも重大な影響を及ぼすものであることから、情報や情報システムなどに係る研究と組織の経営等に係る研究は、連携して行われることが求められる。また、サイバー空間と実空間が融合していることから、情報セキュリティの問題を考えるにあたっては、単に情報システム等の脅威を考えたり、技術的な研究をするのみならず、国際政治、法律、安全保障、危機管理、経済学、心理学等の社会科学的視点も含めさまざまな領域の研究とも連携して行われることが求められる。

こうした総合的な研究が進むことにより、社会全体及び国家安全保障、また個々の組織の事業・業務などにとっての、情報セキュリティに係る脅威やリスクをより体系的・科学的に認識することが可能になる。また、今後発生しうる脅威・リスクを予想し、取るべき対策のオプションやそれぞれの長所・短所の分析を効果的に行うことができるようになるため、リーダーやマネージメント層の取るべきアクションも明確化されると考えられる。

しかしながら、現状では、こうした融合・学際的な領域における分析や研究に従事する人の数が限定的である。また、日本ではセキュリティ製品以外の目に見えない情報等に対する価値や対価について海外と比較して十分になされているとは言い難いとした指摘もある。そのため、今後、こうした融合・学際的な領域の研究を進める研究者等が集まったコミュニティを形成し、積極的に推進していく。さらには、将来の学会化を目指す。

また、社会科学面からの研究の進展のためには実証データの収集・共有が不可欠であるが、日本では、海外と比べ、サイバー攻撃に関する統計値が少なく、適切な対策を立てることが困難な状況にある。社会科学面からの研究のためには、実証データを収集・共有することが継続した研究の進展に寄与するため、社会科学的な観点での研究を実証するための信頼あるデータを収集し、一定の基準のもとに研究者等で共有するしくみが期待される。

さらに、経営学、心理学等の社会科学的視点を含め、幅広い視点から情報セキュリティの研究体制についても関係機関が連携して検討していくことが重要である。

６　情報セキュリティの研究開発における重要分野

情報セキュリティの研究開発の推進方針について、前述の４章、５章で示した。本章では、情報セキュリティ研究開発戦略（2011 年 7 月策定版）で提示してきた、情報セキュリティ関連の研究開発における重要分野を再整理する。今回、再整理するにあっては、次の考え方に基づき行った。

情報セキュリティ関連の研究開発について、民間企業のみによっては十分に実施されていない研究領域がある。このような領域について、産学官が連携するなどにより取り組まれることが重要であり、政府や公的研究機関[4]や大学法人などの役割も重要となる[5]。このような背景も踏まえ、国の施策として推進すべき重要分野や研究テーマを例示する。また、独立行政法人や大学法人などは、法人又は研究者として推進するテーマ等を決定していくものであるが、この重要分野はこれら法人又は研究者の研究テーマ検討時の際の参考としての位置づけも持つ。さらに、テーマ等に対応して、留意すべき点もあることから、これらについても示すこととする。

情報セキュリティ研究開発の重要分野の考え方は、３章～５章を踏まえ、以下のとおりとする。

１．最近の脅威や今後の動向に応じた研究開発の実施
２．社会インフラ、ハードウェアセキュリティ（制御システム等）への対応
３．発展が期待される分野での上流工程からのセキュリティ品質の確保
４．情報セキュリティのコア技術（暗号技術等）の保持

4　情報セキュリティ研究を行う公的研究機関等には、独立行政法人（情報通信研究機構（NICT）、産業技術総合研究所（AIST））や、防衛省の技術本部などがある。

5　情報セキュリティの研究開発は、大学法人や公的研究機関等だけでなく、国内外の民間企業等においても、様々な研究開発が実施され製品・サービス化が行われているところであるが、民間企業における研究開発にも、政府等で支援・取組が必要と思われる研究も多岐にわたり存在している。

上記の重要分野の考え方１について、情報セキュリティ上の脅威については、例えば以下のようなものがある。

表 3　情報セキュリティ上の主な脅威の例

情報セキュリティ上の脅威の例	
a	サイバー攻撃による情報の窃取や破壊、サービス妨害
b	ＩＤパスワードの窃取やなりすまし
c	スマートフォンやパソコン等での悪意あるアプリの増大
d	ソフトウェア脆弱性を狙った攻撃
e	社会システムを構成する、制御システムを狙った攻撃
f	個人情報やプライバシー情報、機密情報の漏えい
g	情報通信システムでの情報の盗聴・傍受
h	インターネットバンキングなどで認証を横取りして 不正な操作をするマルウェア

前述の重要分野の考え方２について、サイバー攻撃の対象が、海外等では社会インフラを構成する制御システムに拡大しており、対策が求められている。

一方、半導体の偽造なども顕在化しており、半導体の偽造防止技術や、ＩＣカードのようなセキュリティデバイスの研究開発も求められている。社会インフラ、ハードウェアセキュリティへの対応として、重要度が高いと思われるものとして、例えば以下のようなものがある。

表 4　社会インフラ、ハードウェアセキュリティへの対応

社会インフラ、ハードウェアセキュリティ（制御システム等）への対応	
i	制御システムセキュリティ
j	セキュリティデバイス

前述の重要分野の考え方３について、今後発展が期待される分野で、特にセキュリティ品質が求められる分野には、例えば以下のようなものがある。

表 5　今後発展が期待される分野

今後発展が期待される分野	
k	医療健康分野（地域医療連携、健康情報の利活用等）
l	次世代インフラ（防災・減災分野でのセンサー情報等）
m	ビッグデータの利活用
n	家電等のネットワーク接続（ＩｏＴ分野）
o	自動車のネットワーク接続（ＩＴＳ分野）

前述の重要分野の考え方４について、情報セキュリティのコア技術として、例えば以下のようなものがある。

表 6　情報セキュリティのコア技術

情報セキュリティのコア技術	
p	サイバー攻撃の検知／防御技術
q	認証技術（バイオメトリクスを含む）
r	情報通信ネットワークのセキュリティ
s	暗号技術
t	制御システムのセキュリティ技術
u	標準化／評価技術

以上の重要分野の考え方を踏まえ、情報セキュリティ研究開発の重要分野を、表７に示す。

表 7　情報セキュリティの研究開発における重要分野

（１）情報通信システム全体のセキュリティの向上	
①	サイバー攻撃の検知／防御
②	ＩＤ連携／認証／アクセス制御
③	ＩＴサービスのセキュリティ（スマートフォン／クラウド等）
④	次世代ネットワークセキュリティ
（２）ハードウェア・ソフトウェアのセキュリティ向上	
⑤	制御システムセキュリティ
⑥	セキュリティデバイス
⑦	ソフトウェアの安全性確保
（３）個人情報等の柔軟管理の実現	
⑧	プライバシー保護／パーソナルデータ利活用のための技術
⑨	フォレンジック等を支援するためのデータ管理・追跡技術
（４）研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	セキュリティ理論体系化／調査研究
⑪	標準化／評価／制度／基盤整備
⑫	暗号技術
（５）発展が期待される応用分野でのセキュリティ確保	
⑬	医療健康分野での情報流通変革に伴い必要となるセキュリティ技術
⑭	次世代インフラで必要となるセキュリティ技術
⑮	ビッグデータにおける情報の秘匿化、暗号化などのセキュリティ技術
⑯	家電、自動車のネットワーク接続で必要となるセキュリティ技術

研究開発を進めるにあたっては、攻撃者によるサイバー攻撃の被害を極小化させるとともに、攻撃者の経済的負担を増大させるなど革新的な取組（いわゆる、ゲーム・チェンジ）に重点を置き、社会を支える基盤として、より安全・安心で、新しい価値を創造できる情報通信システムを実現するための研究開発を重視する。

このとき、情報セキュリティの確保といった従来の狭義の情報セキュリティの視点ではなく、社会全体のリスクの低減に寄与するといった広義の情報セキュリティの確保に重点をおいて対策を検討することが重要である。

（1）情報通信システム全体のセキュリティ向上

近年、国家や企業の機密情報・知的財産を狙った高度なサイバー攻撃が発生しており、複雑化、多様化している。

また、ＩＤ・パスワード認証システムでの不正アクセス、スマートフォンでの不正アプリによる情報窃取などが急増している。

サイバー攻撃の手法は、ますます複雑化・巧妙化する傾向にあるが、サイバー攻撃への対応は後追いとなる傾向があり、根本解決を目指した研究開発がされることが重要である。

また、従来の防御側の対策のみならず、攻撃者に着目したディフェンス技術も重要となっている。

以下、個別のテーマについて説明する。

① サイバー攻撃の検知／防御技術

サイバー攻撃について、サービス不能攻撃や Web 改ざん攻撃などマルウェアを介して行われるものが多くあるが、現状、亜種などウイルス対策ソフトでは検知できないようなマルウェアが日々発生している状況であり、これらのマルウェアによりインターネットバンキングでの不正送金被害や、組織や政府機関等の機密情報を狙った高度な標的型攻撃などが増加している。

サイバー攻撃の検知、解析能力は、国民の財産、国家や企業の機密情報の保護、国家の安全保障上、組織の持続的成長の観点からも重要であり、公的研究機関や大学等でも、産業界とも連携もしながら、研究を行うことが重要となっている。

現在のインターネット環境は攻撃者に有利な状況であり、攻撃に対する後追

い対策では、対策コストの増大を抑えることができない。このため、米国においては、攻撃者に有利な状況を打開するための研究開発を緊急の課題として進めており、我が国においてもサイバー攻撃の検知及び防御の技術の開発を通じて早急に取り組むことが期待されている。

４.（１）でも記載したとおり、サイバー攻撃対処能力の向上のためには、攻撃者やネットワーク利用者、ネットワーク運用者といった多角的な視点のもとで研究開発を行うことが重要である。

攻撃者側の視点として、攻撃者の動向などに着目しながらサイバー攻撃を解析し解析結果に基づく防御方策を検討する必要がある。例えば、ネットワークを介した外部攻撃者の行動観測によるプロファイリングなどを踏まえながらマルウェアを解析することでサイバー攻撃の検知技術を向上させるとともに、解析結果を踏まえて必要となるインシデントレスポンスを確立し、サイバー攻撃への対処能力を向上させる。

また、ネットワーク利用者側の視点として、ネットワーク環境の特性や利用者の行動特性、通信頻度などを解析し、それらの解析結果に基づいた利用者ごとのリスク分析や効率的なサイバー攻撃検知を行うための技術を開発する。
この際、攻撃方法はセキュリティ対策の状況によって動的に変化するため、これを防御する側としても即時的な通信の遮断やネットワーク構成の変更といった動的なセキュリティといった視点も重要である。

分散サービス不能（ＤＤｏＳ）攻撃においては、世界のある地域で発生した攻撃と同種の攻撃が時間をおいて別の地域で発生するなど、ＤＤｏＳ攻撃の検知及び防御には国際的な枠組みによる対処が必要である。そのため、サイバー攻撃、マルウェア等に関する情報を収集するネットワークを諸外国と連携して構築し、サイバー攻撃の予兆を検知し、迅速に対応することを可能とする技術の研究開発・実証が必要である。また、これらの国際的な枠組みの構築を効果的に推進するために、諸外国とのネットワークセキュリティ分野における技術協力を推進することが重要である。

さらに、サイバー攻撃の検知においては、最新のサイバー攻撃を収集し、解析を行うためのプラットフォームとしての環境の整備が重要であり、実組織のネットワークを模擬した実証環境の構築や、大規模ネットワーク観測システムやマルウェア自動解析システムによりサイバー攻撃をリアルタイムに観測・分析するシステムの構築が期待される。

マルウェア等の検知については、民間のウイルス対策ソフト等で十分な検知がされるようになることが望ましいが、近年、亜種などの発生により検知できないマルウェアが増加している状況にある。
そのため、大学や公的研究機関等の研究においても、マルウェア等のサイバー攻撃の検知・解析能力を高める研究を行うことが期待される。

また、規模の大きいサイバー攻撃（例：ＣｏｄｅＲｅｄやＮｉｍｄａのようなタイプの拡散性の高い悪性プログラムや、複数政府機関等への無差別ＤｏＳ攻撃、韓国で発生したような大規模サイバー攻撃によるコンピュータ障害等）の発生などに備え、事象発生の事前や事後に防御できるような技術が期待される。

② ＩＤ連携／認証技術／アクセス制御

ＩＴの利活用が進む中で、なりすましを防ぎ、互いに信頼できる相手との通信を確保するための仕組みとして認証技術がある。認証技術の活用が進むにつれ、利用者においてもＩＤ・パスワードなどの多くの認証要素を管理する必要があるなど多くの労力が生じており、また、攻撃者においても認証の仕組みを悪用したサイバー攻撃を行うなど、安全かつ利便性の高い認証を実現が求められている。認証技術においては、民間企業等においても様々な研究開発や製品・サービス化が行われているが、マイナンバー制度やトラストフレームワーク等の制度の動向も踏まえて、便利なＩＴ社会を実現するため、大学や公的研究機関等の研究者等が取り組むべき課題も多く存在していると考えられる。例えば、人の認証に関して、現状、システム毎に、使用するＩＤ・パスワードなどが増加し、利用者の大きな手間となっているが、複数システム間でのＩＤ連携など子供や老人などの情報リテラシーの低い者にも優しいＩＴ環境を実現するするとともに、なりすまし被害にあいにくい認証技術が期待される。

なお、認証技術の開発や適用シーンの考慮にあたっては、認証技術を利用する個人の行動科学の観点からの研究、事業者の事業リスクの認知や意思決定についての経営的な視点での研究も、技術面からの研究に加えて考慮すべきである。

生体認証について、日本はバイオメトリクスの要素技術に強みを持っており、この強みを維持するためにも、統合システムの部品となるバイオメトリクス認証技術の適合性評価を行う国際的なフレームワークにおいて、イニシアチブを取っていくことが期待される。
また、確実な本人確認の技術として、生体認証などを活用したＩＴによる認

証の仕組みを開発し、利活用を進めることで、利便性の高い本人認証が可能となることが考えられる。

モノの認証においても、ＩｏＴの拡大に伴い様々なモノがネットワークで接続される中で、Ｍ２Ｍの活用が期待されるところ、情報セキュリティ上の機密性・完全性が確保されなければ、なりすましなどのサイバー攻撃も見込まれることから、Ｍ２Ｍの認証の情報セキュリティ技術の開発・実証を行うことで、更なる普及・展開を図る。

アクセス制御について、例えば、組織や個人の利用者において、通信先を許可された範囲に制限するなど、不正通信のリスクを軽減できるようなアクセス制御技術の開発が期待される。
その技術に必要となる、不正なＩＰアドレスやドメイン名、ＵＲＬをブラックリストとして管理するような環境整備も期待される。

具体的取り組みの一例として、組織や個人の利用者におけるマルウェア感染等を防止し、不正通信のリスクを軽減するために、利用するアプリケーションやアクセス先を制御する技術等が求められる。具体的には、組織において、標的型攻撃との関係性の認められないアプリケーションに利用を制限することで標的型攻撃を防御するための技術の開発を行う。また、個人の利用者において、マルウェアを配布するサイトやフィッシングサイト等の悪性サイトの情報（ＩＰアドレスやＵＲＬ等）を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする利用者に対する注意喚起を実施することでマルウェア感染等を防止するための取組について、国際的な展開を視野に入れつつ推進する。

③ ＩＴサービスのセキュリティ（スマートフォン／クラウド等）

近年、スマートフォン、クラウドサービス、ＳＮＳ、インターネットバンキングなど様々なＩＴサービスが近年普及している。

しかし例えば、スマートフォンでの不正アプリの増加や、インターネットバンキングなどで認証を横取りして不正な操作をするマルウェア（Man-in-the-Browser 攻撃[6]）などが発生してきている。
ＩＴ利用者の財産やプライバシーを保護するため、スマートフォンのセキュリティを向上させる技術や、利用者がアプリの安全度を可視化できるような技

6 利用者の PC に感染したマルウェアがウェブブラウザを乗っ取り、正しいセッションに便乗して不正操作を紛れ込ませる攻撃。例えば、インターネットバンキングにおいて、利用者による正規処理の裏で送金先を書き換える等の不正処理を行うもの。

術・制度が期待される。

また、クラウドサービス利用についても、セキュリティ上の課題やリスクが残存しており、安心した利用の妨げの一因となっていることが考えられる。

一方、インターネットネットバンキングや電子政府、電子申請システムなどにおいて、利用者認証を強化しても、認証を横取りして不正な操作をするマルウェア（Man-in-the-Browser 攻撃）などは防ぐことができないといった課題もある。このような攻撃に対しても安全に取引できる対策、技術開発が期待される。

これらのセキュリティ技術開発は従来までも推進されてきたものもあるが、セキュリティ上の課題はまだ残存しており、また新しいＩＴサービスも生まれている。公的研究機関や大学、研究者等が取り組むべき研究について継続して行われることが期待される。

④ 次世代ネットワークセキュリティ

次世代ネットワークの技術の確立、新世代ネットワークの実現を目指しており、それに向けて必要となるセキュリティアーキテクチャや要素技術の研究開発が期待される。ＩＰｖ６への移行に備え、必要な技術開発・検証も期待される。

さらに、インターネットを基盤として実現される社会システムでは、クラウド化、仮想化、端末のユビキタス化が進展し、リアルタイムセンシング機能の強化、位置情報等を活用したコンテクスト・アウェア化（センサーを用いてリアル空間の状況をコンピュータ内に能動的に収集・処理を行う）が進んだＣＰＳ（Cyber-Physical-System)が実現すると考えられている。ＣＰＳでは、現実世界と情報通信システムの結びつきが今まで以上に強まったシステムになる。このため、実世界とコンピュータを繋ぐセンサーや制御機器を構成要素とするシステムには高い信頼性・セキュリティを実現できる技術が期待される。

様々なセンサーが家庭や職場、社会システムなどに設置され、センサーネットワークや、バックボーンを介さないアドホックネットワークの利用などが進むと考えられると考えられているが、その情報セキュリティ技術は未だ十分に確立されておらず、利便性と安全性のバランスを考慮した情報セキュリティ基盤の確立が期待される。

このためセンサーネットワークの情報セキュリティ基盤技術や、アドホックネットワークにおける利便性と安全性のバランスを考慮した情報セキュリティ基盤技術等の研究開発が重要となってくる。例えば、端末間の通信におけるネットワーク・サービスの状況や脆弱性について、セキュリティ知識データベースのデータを照合しながら、その通信に係るリスクを評価し、適切な情報セキュリティ設定を導出する技術が考えられる。

（2）ハードウェア・ソフトウェアのセキュリティ向上

近年、社会インフラを構成する制御システムなどをターゲットにしたセキュリティ攻撃のリスクも国外で顕在化しており、国民生活や国家の安全への脅威も現実的なものとなってきている。

安全で安心なＩＴ社会を実現するには、ハードウェア・ソフトウェア[7]のセキュリティ向上も重要となる。

⑤ 制御システムセキュリティ

近年、制御システムをターゲットにしたセキュリティ攻撃のリスクも国外で顕在化しており、制御システムにおけるセキュリティ対策の必要性が高まっている。

発電所やガスプラントなど、重要インフラの制御システムに対するサイバー攻撃への対処は、国家の安全保障、危機管理上重要な課題である。

また、海外では、制御システムセキュリティに対する国際規格の整備が進み、これに基づく適合性評価制度が確立されてきており、インフラシステム輸出に対する貿易障壁となる可能性が出てきている。

そのため、制御システムに関するセキュリティの研究開発や認証制度の確立を推進する。

⑥ セキュリティデバイス

ＩＣカード、偽造防止機能付き半導体など、セキュリティ機能を備えたデバイス（セキュリティデバイス）が多くの IT 製品で利用されている。

例えば、高度なセキュリティデバイスを活用することで、インターネット上における確実な本人認証を容易に実現したりすることが期待される。

民間企業でも様々なセキュリティデバイスを開発されているが、大学や公的研究機関等の研究としても、必要な研究開発が期待される。

---

7 ハードウェアとは、コンピュータを構成する電子回路や周辺機器など物理的なものを指す。例えば、電子回路、ＩＣカードやＵＳＢデバイスのようなものを含む。

但し、セキュリティデバイスの研究開発にあたっては、民間企業や個人、セキュリティ製品市場などへ悪影響を与えないように留意する必要がある。

⑦ ソフトウェアの安全性確保

インターネット環境におけるソフトウェアの脆弱性により、情報漏えいや改ざんが発生したり、脆弱性対処のための労力が発生したりする問題は長年継続している。ソフトウェアの安全性評価技術、脆弱性を検知したり、脆弱性を作りこまないためのソフトウェア開発技術など、ソフトウェアの安全性確保に関する研究について、継続して実施することが期待される。

（3）個人情報等の安全性の高い管理の実現

⑧ プライバシー保護／パーソナルデータ利活用のための技術

今後、ＩＴの利活用が進むにつれ、様々なデータの利活用が盛んになることが見込まれるが、データの利活用、特にパーソナルデータの利活用においては、個人情報の保護、プライバシーの保護に十分配慮する必要がある。ＩＴ総合戦略本部において行われている制度見直しの動向も踏まえながら、十分な安全性を確保しつつも利便性の高い技術を開発することが期待されている。

例えば、プライバシー情報については現状、提供するか、提供しないかという１か０かであるため、個人においてもプライバシー情報を適切にコントロールすることが難しく、データ利用者においてもプライバシー情報を適切に利用することが難しい。プライバシー情報の適切なコントロールが実現すれば、情報の有効活用によるメリットを享受することが可能になる。このため、プライバシー情報等の積極活用と保護のバランスなど、多様性に対応した自律管理性を向上する技術が期待されている。

ほかにも、位置情報やライフログなどのプライバシー情報を適切に利用するためには、プライバシー保護レベルやポリシーを柔軟に設定するシステムの開発、プライバシーを保護したまま有用なデータを計算するための秘密計算や匿名化技術、プライバシー保護データマイニング等の基礎的研究が考えられる。

なお、プライバシー保護については、各個人の認識度合が多大な影響を及ぼすものであり、そのような点も考慮していく必要がある。ＥＵでは、大規模なプライバシー意識調査を行う、プライバシー保護に関する制度を早くから取り組むなどしており、こういった海外での先進事例も活用していくことが期待さ

れている。

⑨ フォレンジック等を支援するためのデータ管理・追跡技術

個人にとってプライバシー情報の漏えいが大きな問題であると同じように、政府にとっては、国家機密の情報漏えいや知的財産の国外流出が発生することは大きな問題であり、これらを防止・抑止したり、問題発生時に追跡するための技術開発が求められている。ネットワークを介した情報漏えい事件が増加傾向にあることから、漏えい先を突き止めるための追跡技術や、情報の改ざんや情報漏えいに関与したものを特定するための証拠データの収集技術が望まれている。

ただし、これらの技術開発にあたっては、まず、通信の秘密などの法制度との関連性考慮や、プライバシー侵害を行わないような配慮が必要である。

（４）研究開発の促進基盤の確立と情報セキュリティ理論の体系化

⑩ 情報セキュリティ理論の体系化／調査研究

現在の情報セキュリティの研究開発は、個々のリスクに対応する対策のノウハウ集になっている側面が強いため、情報セキュリティ理論の体系化が期待される。

また、技術面だけでなく、情報セキュリティに係る海外の動向、社会科学（国際情勢、法律、経営学、心理学、リスク管理など）など他分野と連携した研究や分析、ＩＴ利用者、システム運用面の視点も含めた分析なども重要である。

研究テーマは多岐にわたるが、一例としては以下のようなものがある。

・情報セキュリティに係る海外の動向、国際情勢分析
・ＩＴリスクに関する理論から実務までの体系化
・ＩＴ分野以外のリスク管理と連携した、統合的なリスク管理
・非常時（災害発生時や緊急時）における個人情報などの取扱いに関する研究、リスクコミュニケーション
・経営層向けの最適なセキュリティ対策投資効果の判断材料に資する研究

これらについては、民間企業、政府、大学、公的研究機関等が分担・連携して調査研究が行われることを期待する。

また、調査研究や分析サービスは、民間企業等でもサービスが充実されることを期待する。

⑪ 標準化／評価／制度／基盤整備

研究開発や技術開発にあたっては、情報セキュリティに係る技術の標準化、国際標準化、プロトコルの開発、ソフトウェアやＷｅｂサービスなどのセキュリティ評価体系の確立、法律面や制度面の分析や整備、情報セキュリティ研究や検証を推進するうえでのテストベッドや研究データなどの環境整備も重要となってくる。

これらの取り組みは、情報セキュリティ技術の効果的な社会適用、国際貢献や国際展開、産業活性化の観点からも重要である。

なお、民間企業単独での推進は難しい側面もでてくるため、政府や公的研究機関等は積極的に支援する必要がある。

⑫ 暗号技術

暗号技術については、国の機密情報の保護をはじめ、インターネットを通じた商取引等様々な分野における基盤として用いられており、安全な通信を確保し、情報通信技術の利活用を促進するためにも、暗号が危殆化する前により強固な暗号へ移行することが不可欠である。暗号技術については、ＣＲＹＰＴＲＥＣを中心に取組が進められているところであるが、引き続き暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討など暗号技術の強化に向けた取組を進める必要がある。

情報理論的に安全な暗号技術は、従来主流の計算量的暗号技術に対比される技術である。近年、重要インフラの制御システムを狙ったマルウェアが登場しており、制御システムのセキュリティ対策の必要性が高まっている。ＤＥＳ、ＲＳＡなどの計算量的な暗号技術の場合、計算機の処理速度の向上に伴う危殆化の問題が付きまとう為、制御システムの稼働期間（十数年の長期）に渡って、安全性を保障することはできない。

また、ＩｏＴの拡大に伴い、センサー機能を持った機器が家庭やオフィスに配置され、ネットワークに接続されるようになってきており、これらのＭ２Ｍのセキュリティ対策が求められている。情報理論的な暗号は、線形演算で構成でき高速処理が可能となるため、計算資源の小さい組み込みシステムへの適用が可能と考えられる。

情報理論的に安全な暗号技術を実用化するためには、組込みシステムへの導入に関する研究も重要となる。車載コンピュータ、制御系コンピュータ、電力システムなど、システムごとにリソースやリアルタイム性の制約を考慮した方

式の研究開発が期待される。

また、情報理論的に安全な暗号技術の１つである量子暗号技術では、大きな秘密鍵を事前に共有する仕組みが重要となり、その手段として量子通信等が有望とされている。特定環境における量子通信の実現は、１０～２０年程度の研究課題とされており、国際的な成果も活用して推進することが効率的である。

（５）発展が期待される応用分野でのセキュリティ確保

⑬ 医療健康分野での情報流通変革に伴い必要となるセキュリティ技術の開発・検証

医療健康分野では、在宅医療・介護の推進や、カルテ情報の病院間共有などがより進むと考えられる。在宅医療・介護においては、タブレット端末を活用した診察や、計測した患者のデータを無線を用いて自動的に登録するシステムなどが期待されるところ、これらの情報を安全に取り扱う情報セキュリティ技術や、ゲノム情報などのセンシティブデータの機密性や完全性を高めるための技術が期待される。

また、緊急時（救急治療や大規模災害時）と平常時では、個人情報や医療情報の取り扱いを変えるべきとの指摘もあり、このような検討と研究を進めることも重要である。

⑭ 次世代インフラで必要となるセキュリティ技術の開発

次世代インフラでは、例えば、センサーネットワーク、M2M デバイスの活用などにより、情報の収集やコントロールすることが考えられる。次世代社会インフラで扱う情報や情報システムの機密性・完全性・可用性が損なわれると、社会の安全や人の生命にもかかわる可能性があることから、次世代インフラのセキュリティを確保する技術が期待される。

⑮ ビッグデータにおける情報の秘匿化、暗号化などのセキュリティ技術の開発

ビッグデータを用いた分析と、利活用技術の利用が進んでおり、また期待されている。ビッグデータにおける情報セキュリティを確保するための技術はまだ十分とは言えない状況である。

民間企業等でも、様々な技術開発が行われているが、国の研究機関等でも、官民連携した標準化や制度づくり、必要な技術開発を行うことが期待される。

⑯ 家電、自動車のセキュリティ技術の開発

家電、自動車などもネットワーク接続等が進んでいくことが考えられ、それに向けて必要となるセキュリティ技術が開発されることが求められる。

官民連携した標準化や制度づくり、必要となる技術開発を行うことが期待される。

7　おわりに

本「研究開発戦略」では、情報セキュリティの研究開発に係る現状認識、研究開発戦略見直しにあたっての課題、研究開発取組方針、研究開発の効果・成果を高めるための方策等、研究開発における重要分野について記載した。

今後、研究開発戦略に沿って政府や公的研究機関等での情報セキュリティ研究開発が推進されるとともに、大学や企業等における情報セキュリティ研究開発においても、産学官で互いに連携して推進され、我が国の情報セキュリティ研究開発能力が高まることが期待される。

情報セキュリティはＩＴの利活用を推進するうえで、重要となるものであり、今後のＩＴ自体の発展や、社会インフラ等に付属するＩＴの利活用の促進に必要な情報セキュリティの技術、そのために必要となる研究開発が我が国で実施されることが期待される。

研究開発の成果は短い期間で出るものではなく、長期的に取り組まなければならない課題である。特に、研究開発を支える研究者の育成や、我が国のコア技術の維持については、最終的には日本の社会全般の制度・意識等様々な事項と関連して横断的取組が必要なものである。このため、政府としては産学官の関係機関、関係者が共通の認識、意識をもって、情報セキュリティという観点のみならず、環境の変化に留意しつつ、総合科学技術会議やＩＴ総合戦略本部等の他の関連施策とも連携を図りながら、総合的に積極的な施策を推進していくこととする。 また、研究開発戦略に基づき推進する施策の進捗状況について技術戦略専門委員会等においてフォローアップを実施し、必要な見直しを行っていく。

これらの取組により、我が国の情報セキュリティの研究開発が促進されるとともに、研究開発の成果の活用により我が国発の技術のグローバルな発信等我が国の産業の活性化につながり、我が国の産業競争力のさらなる向上が実現されることを強く期待する。