サイバーセキュリティ戦略

［案］

～世界を率先する強靭で活力あるサイバー空間を目指して～

平 成 ２５年　　月　　日

情報セキュリティ政策会議

目次

はじめに

情報セキュリティ問題への取組を抜本的に強化することを目的に、2005年4月に内閣官房に情報セキュリティセンター（NISC）が、同年5月に高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）に情報セキュリティ政策会議がそれぞれ設置されて以来、8年が経過した。

この間、情報セキュリティ政策会議は、「第1次情報セキュリティ基本計画」、「第2次情報セキュリティ基本計画」及び「国民を守る情報セキュリティ戦略」を決定し、情報の自由な流通の確保と的確なリスク対応のバランスに配意しつつ、我が国における情報セキュリティ水準の向上を図ってきた。

情報セキュリティを取り巻く環境変化は、極めて急速である。前戦略策定後3年間で、リスクは甚大化し、拡散し、グローバルレベルのものとなった。国家や重要インフラに対する「サイバー攻撃」が現実のものとなり、「国家安全保障」や「危機管理」上の課題となっている。今や、国家や重要インフラの防護に最善の措置の導入が不可欠となっている。

間もなく、Internet of Things と呼ばれる、あらゆるものがインターネットに接続される時代を迎える。あらゆるものが情報セキュリティ上のリスクを抱える時代である。また、インターネットに接続されない制御システムにおいても、同様にリスクが高まっている。すなわち、国民生活のあらゆる側面において、情報セキュリティ対策が不可欠の時代となった。情報セキュリティは「国民生活の安定」や「経済発展」に直結する課題となっている。

我が国は「世界最先端のIT国家」の構築に取り組んでいる。世界最先端のIT国家には、それにふさわしい「安全なサイバー空間」を実現しなければならない。急速に変化する環境の中で安全なサイバー空間を構築するには、これまで同様個々の主体における情報セキュリティの確保が不可欠であると同時に、サイバー空間にかかわるあらゆる主体の貢献が必要となっている。

このように、従来の「情報セキュリティ」確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確化するため、本戦略の名称は「サイバーセキュリティ戦略」とした。

本戦略では、これまでとは次元を変えた取組が必要との認識から、さまざまな新たな課題を提示している。これらを含めて本戦略が着実に実施され、「世界を率先する強靭で活力あるサイバー空間」を有する「サイバーセキュリティ立国」が速やかに実現されることを期待する。

1. 環境の変化

(1)サイバー空間の拡大・浸透

①サイバー空間と実空間の「融合・一体化」の進展

情報システムや情報通信ネットワーク等により構成され、多種多量の情報が流通するインターネットその他の仮想的なグローバル空間である「サイバー空間」が、急速に拡大し、実空間に浸透している。今や、サイバー空間は、人々の日常生活、社会経済活動、行政活動等のあらゆる活動に必要不可欠な頭脳・神経系となっており、サイバー空間と実空間の「融合・一体化」が進展している[1]。

サイバー空間の拡大・浸透は、情報通信技術の普及・高度化と、当該技術に係る利活用の進展の結果生じている。すなわち、ブロードバンド基盤の国内全域への整備、スマートデバイス、IPv6、M2M[2]・センサーネットワーク、クラウドコンピューティングサービス等の普及・高度化[3]を背景に、これらが電子商取引、医療、教育、交通、社会インフラ管理、行政等の多様な分野において利活用されている。

サイバー空間は、我が国の成長力強化にとって不可欠であり、今後も一層拡大・浸透していくと考えられる。例えば、成長力強化にとって重要な安全・便利で経済的な次世代インフラや、クリーンかつ経済的なエネルギー需給を実現するためには、オープンデータやビッグデータを利活用したITS[4]やスマート

---

[1] 例えば、総務省「平成24年版情報通信白書」(以下「情報通信白書」。)では、「インターネットがグローバル社会における社会経済活動に不可欠の基盤となる」、警察庁「平成24年版警察白書」では、「インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着する」、防衛省「平成24年版日本の防衛 防衛白書」では、「軍隊にとって情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、IT革命によって情報通信ネットワークへの軍隊の依存度が一層増大している。」とされている。

[2] Machine to Machine。ネットワークに繋がれた機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステム。例えば、各種センサー・デバイス(情報家電、自動車、自動販売機、建築物、スマートフォン等)を、ネットワークを通じて協調させ、エネルギー管理、施設管理、経年劣化監視、防災、福祉等の多様な分野のサービスを実現するもの。

[3] 例えば、独立行政法人情報処理推進機構(以下「IPA」。)「情報セキュリティ白書2012」では、「システム環境も、ここ数年で大きく変化している。新たなデバイスの登場、制御系システムのオープン化、また、クラウド・コンピューティングのようにサービス構造にも変化が起こって」いるとされている。

[4] Intelligent Transport System(高度道路交通システム)。人と車両と道路との間でネットワーク化することにより、道路利用者の利便性向上、交通事故・渋滞の解消、交通ネットワーク管理の最適化等を目指すもの。既に、ナビゲーションシステム、自動料金収受システムが普及。今後、車車間・路車間通信による安全運転システム、自動運転等の実用化等が期待されている。

グリッドが必要である。これらを構成する情報システムや情報通信ネットワーク等は、サイバー空間の更なる拡大・浸透をもたらすことになる。

また、サイバー空間については、グローバルにもますます拡大・浸透していくことが期待されており、経済成長及びイノベーションを推進し、社会的課題を解決等する必要不可欠なものとして、国家の成長を牽引する力に世界的に注目が高まっている[5]。

②サイバー空間を取り巻く「リスクの深刻化」

サイバー空間については、匿名性が高く、痕跡が残りにくい、また、地理的・時間的制約を受けることが少なく、短期間のうちに不特定多数の者に影響を及ぼしやすいといった特性を有している。

このため、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃[6]等の、いわゆる「サイバー攻撃」の脅威が増大している。

初期のサイバー攻撃には、自己顕示欲、見せしめ、嫌がらせ等を目的とした愉快犯[7]による目立つ脅威が多かった。しかしながら、次第に金銭や示威を目的とするもの[8]が出現し、最近では国家や企業の機密情報等を窃取しようとするもの[9]、重要なデータやシステムを破壊しようとするもの[10]が顕在化している。さらに、海外においては、軍事行動との連携が現実のものになっているといわれるサイバー攻撃が指摘されるとともに、多くの外国軍隊がサイバー空間における攻撃能力を開発しているとされ、また、情報収集のために他国の情報通信

---

[5] 例えば、G８ドーヴィル・サミット首脳宣言（2011 年５月）では、「インターネットは、世界中至るところで我々の社会、経済及びそれらの成長に不可欠なものとなっている。（中略）インターネットは、世界経済、その成長及びイノベーションの主要な推進力となっている。」と確認されている。

[6] Distributed Denial of Services 攻撃（分散サービス不能攻撃）。

[7] 例えば、2000 年代前半に流行した、メールで感染を広げ、パソコン内のデータを破壊する「loveletter（ラブレター）」。

[8] 例えば、2012 年６月頃、いわゆるハクティビストより違法ダウンロード刑事罰化に関する著作権法の改正を批判する声明が出され、行政機関、政党、関係団体等において、ウェブサイトの改ざんや DoS 攻撃等の被害が発生した。

[9] 例えば、2011 年９月以降、議院、行政機関、防衛関連企業等への標的型攻撃によるウイルス感染が発覚した。

[10] 例えば、2012 年８月頃、海外において、感染したコンピュータのマスターブートレコード（MBR）を改ざんするなどの手法を使って起動不能にさせる「Shamoon（シャムーン）」によるサイバー攻撃が発生した。

ネットワークへの侵入が行われているとの指摘もある。

サイバー攻撃の手法についても、複雑・巧妙化してきている。例えば、ウェブサイトの改ざんやDDoS攻撃によるオンラインサービスの停止[11]といったもののほか、ウェブ感染型ウイルスによるドライブ・バイ・ダウンロード攻撃[12]、インターネット等外部との接続を持たないクローズドな制御系ネットワークに対するUSBメモリ等経由による攻撃[13]、マルウェアがウェブブラウザを乗っ取りその通信を改ざん等するMITB攻撃[14]、いわゆる「やりとり型」[15]といったソーシャルエンジニアリングの活用やゼロデイ脆弱性等を組み合わせた標的型攻撃などが出現してきている。これらの中には、国家レベルの関与が必要と思われる高度の技術と計画性が指摘されているものもある。

また、サイバー攻撃の対象となり得る範囲も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まで広がってきている。個人における複数端末の所有やスマートフォン等のスマートデバイスの急速な普及、家庭における外からの遠隔操作が可能な情報家電等の普及、職場におけるBYOD[16]やコピー機等の複合機等の利用、店舗におけるPOS端末や防犯カメラ等の設置、社会インフラ等の施設におけるセンサー等の活用など、情報通信機器が様々な人やモノ、場所へ分散してきている。

我が国では、これまでも、自然災害や事故による機器の損壊や、正当な使用者によるシステムの誤操作等により、情報の流出やシステムの誤作動などが引き起こされるリスクとともに、サイバー犯罪への対処やサイバー攻撃への対応を進めてきたところである。しかしながら、サイバー攻撃に係るリスクは、その目的や手法等の変化により、従来の想定をはるかに超えた水準まで高まってきて

---

11 例えば、2012 年 9 月頃に発生した、政府機関等に対するウェブサイト改ざん及び DDoS 攻撃。
12 例えば、2009年から2010年にかけて猛威を振るった「Gumblar（ガンブラー）」等、ウェブブラウザやOS等の脆弱性が狙われ、ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる攻撃。
13 例えば、2010 年 11 月のウラン濃縮施設へのサイバー攻撃等で使用された「Stuxnet（スタックスネット）」は、インターネット経由のほか、感染したコンピュータに接続された USB メモリ経由でも発症が可能であり、インターネットから隔絶されたスタンドアローンのネットワークに対しても侵入可能。
14 Man In The Browser 攻撃。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、オンライン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。
15 最初から標的型メールを送付するのではなく、業務との関連を装った通常のメールのやりとりを何通か行い、より自然な状況を装った後に標的型メールを送付する手口。警察庁「平成 24 年中のサイバー攻撃情勢について」（平成 25 年 2 月 28 日）。
16 Bring Your Own Device。企業等において、従業員が私用で使っているスマートフォン等の情報端末から企業等の情報システムにアクセスし、必要な情報を閲覧・入力する等、私物の情報端末を業務で利用すること。

いる。とりわけ「甚大化するリスク」、「拡散するリスク」、「グローバルリスク」として顕著に進行し、「リスクの深刻化」という新たな局面を迎えており、我が国の安全保障・危機管理に影響を及ぼすとともに、国際的な競争力を揺るがし、国民に多大な不安をもたらす恐れが生じている。

【甚大化するリスク】

国の安全及び国民の生命・身体・財産に甚大な被害をもたらす恐れがあるリスクが出現している。我が国においては、国家機関、防衛産業、重要インフラ事業者等及び研究機関などから機密や技術情報等を窃取することが目的とみられる標的型攻撃の脅威の顕在化も指摘されている[17]。

こうした被害においては、発覚した時点で、既に数年前から情報が窃取されていたことが判明した事案[18]もあるなど、被害者はその攻撃や被害そのものを認知していないこともある。さらに、サイバー攻撃による被害が認知された場合であっても、更なる被害の拡大、評判や株価等への影響を回避するため、公表されていない事案もあると考えられる。すなわち、今明らかとなっているものは氷山の一角であって、国家や企業の存続にも係る重要な情報が今も窃取され続けている可能性もある。

海外においては、交通メッセージを表示する信号機システムに対するサイバー攻撃[19]や、複雑・巧妙さから国家レベルの組織の関与も疑われている基幹インフラの制御系システム等に対する高度なサイバー攻撃も発生しており、大規模な社会的混乱等を引き起こされるリスクが現実の問題となっている。

今後は、通信インフラにおけるSDN[20]、交通インフラにおけるITSや電力インフラにおけるスマートグリッドの普及等により様々な社会インフラがネットワークに常時接続され、ソフトウェアにより管理・制御される状態へ進展していくと考えられる。これらにおけるソフトウェアの脆弱性等を狙うサイバー攻撃により、通信障害、交通混乱やブラックアウトといった事態が発生し大規模な社会的混乱

---

17 例えば、脚注９のほか、最近では、行政機関において TPP 関連情報の流出の可能性が指摘された事例、重要インフラ関係事業者における技術情報等の窃取の可能性が問題とされた事例や宇宙関連の航空研究開発を行う独立行政法人における宇宙ステーション関連の仕様情報等の窃取の可能性が問題とされた事例。

18 例えば、行政機関の職員が使うパソコンが数年間、ウイルスに感染し情報が漏洩していた事例。

19 例えば、2009 年 1 月、システムの脆弱性に対するサイバー攻撃により、アメリカの複数州における信号機のメッセージが「Zombies Ahead（ゾンビ注意）」に変更された事例。

20 Software Defined Networking。ソフトウェアにより仮想的なネットワークを作り上げる技術。物理的に接続されたネットワーク上で、 別途仮想的なネットワークの構築が可能。

や人の生死に直接的な影響をもたらすことも可能性として想定される[21]。

【拡散するリスク】

サイバー空間を取り巻くリスクが甚大化すると同時に、リスクが急速に拡散している。スマートフォン等の国民への急速な普及[22]、M2M・センサーネットワークの拡大、あらゆるモノがインターネットに接続され得る状態（Internet of Things）の出現等により、サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで行き渡ることによるリスクの拡散が進行している。

常時、電源が入り、インターネットと接続状態のままで携帯されるスマートフォン等の高度な処理機能等を有するスマートデバイスが、一般利用者を中心に、急速に普及している。これらについては、公衆無線LAN等による通信路を利用することや、OS構造上の制限によりセキュリティ対策ソフトによる対応に限界があること等により、利用者に関する位置情報、電話帳情報や会話情報等が不正アプリにより外部へ送信される等の事案[23]が発生している。オフィスにおいても、スマートフォン等のBYODの普及により、同様の脅威が発生している。

また、M2M・センサーネットワークの普及により、家電、自動車、コピー機等の複合機、防犯カメラ等のモノにもリスクが拡散している。これまでネットワークに接続されてこなかった機器がインターネットに接続され、人を介在しない情報交換により制御等される結果、これらに対するサイバー攻撃により予期せぬ動作が起きる恐れがある。

例えば、外国政府機関等に対するDDoS攻撃[24]において、我が国のコンビニエンスストアに設置された防犯カメラが踏み台となっていたと指摘されている事案などがある。また、インターネットに接続された家電や自動車から家庭内の

---

[21] 産業制御システムの一種であり、コンピュータによるシステム監視とプロセス制御を行うSCADA（Supervisory Control And Data Acquisition）を始めとする制御システムにおけるインシデント数は年々増加傾向にあり、国内外における情報セキュリティ事故の被害例も報告されている。IPA「重要インフラの制御システムセキュリティとITサービス継続に関する調査報告書」（平成21年3月）、経済産業省「サイバーセキュリティと経済 研究会 報告書 中間とりまとめ」（平成23年8月5日）。

[22] スマートフォンの世帯普及率については、平成23年末において、対前年比約20ポイント増となる約30%と急速に普及が進んでいる。総務省「平成23年通信利用動向調査」（平成24年5月30日。以下「通信利用動向調査」。）。

[23] スマートフォンについては、不正課金、管理者権限奪取、無断で電話を発呼、遠隔操作による通話の盗聴及びデータの窃取、利用者の電話帳に登録された個人情報の外部への送信、位置情報を無断で第三者に知らせるなどのマルウェアが確認されている。総務省「スマートフォン・クラウドセキュリティ研究会最終報告」（平成24年6月29日）。

[24] 2011年3月に韓国で発生した政府機関等の40のウェブサーバに対するDDoS攻撃事案。

生活関連情報や走行場所等の位置情報などがサイバー攻撃により流出する恐れや、オフィスにおいて、コピー機等の複合機が営業情報等の情報窃取の拠点になる恐れ[25]も指摘されている。

さらに、インターネットに接続された情報システムのみならず、情報系ネットワーク等の外部ネットワークと切り離されたクローズドな独立系システムもサイバー攻撃の対象となっている。例えば、基幹的なインフラの制御系システムに対して、USBメモリを媒介してマルウェアに感染し、インフラにおける機器を稼働不能とすることも現実の問題となっている[26]。

以上の攻撃対象の広がりのみならず、サイバー空間においては、攻撃する者の範囲も拡大している。資金や知識がない個人でも高度なサイバー攻撃が容易に可能な攻撃用ツールが流通しており、専門家でなくともサイバー攻撃を行うことが可能な環境となっている。

【グローバルリスク】

サイバー空間を取り巻くリスクは、ボーダレスに進行している。インターネット利用者は世界人口の3分の1[27]となっており、新興国や途上国等も含め、グローバルに普及し続けている。我が国は、このようなサイバー空間に実空間のあらゆる活動が依存するようになっていることから、国境のないグローバルなリスクへの一層の対応が求められる。

例えば、我が国においては、海外において発生した外国政府機関等に対するDDoS攻撃において、一般個人の所有する家庭用PCが踏み台となり攻撃指令サーバに仕立てられた事案[28]が発生するとともに、海外で発生した大規模サイバー攻撃に使用されたとされる不正プログラムが、その被害発生と同時期に我が国においても確認されている[29]。また、海外における複数のノード等を

---

[25] IPA「2012年度デジタル複合機のセキュリティに関する調査」報告書（平成25年3月12日）。
[26] IPA「『新しいタイプの攻撃』に関するレポート」（平成22年12月17日）。
[27] 2011年において、世界のインターネット利用者は22.65億人であり、全人口の32.5%を占めている。ITU Statistics: Individuals using the Internet per 100 inhabitants, 2001-2011, & Global numbers of individuals using the Internet, total and per 100 inhabitants, 2001-2011。
[28] 2011年3月の韓国における政府機関等40のウェブサーバに対するＤＤｏＳ攻撃において、一般個人による家庭用ＰＣ等が踏み台としてサイバー攻撃に使用されていた。警察庁「３月の韓国政府機関等に対するサイバー攻撃への対応について」（平成23年9月22日）。
[29] IPA「コンピュータウイルス・不正アクセスの届出状況及び相談受付状況【2013年第１四半期（１月～3月）】（平成25年4月16日）によると、「韓国への大規模サイバー攻撃に使われたとされる不正プログラム Trojan/MBRKill（届出名：Trojan.Jokra［届出件数２件／検 知件数３個］）の届出が2013年３月に寄せられました。この不正プログラムに感染すると、コンピュータのハ

経由する高度匿名化技術が悪用され、遠隔操作ウイルスに感染し成りすまされたPCの所有者が誤認逮捕された事案が発生している[30]。

海外では、企業秘密等の窃取が狙われた標的型攻撃に外国政府の関与が疑われている問題も顕在化している[31]。今後、我が国に対しても外国政府が関与するサイバー攻撃が、いつ発生してもおかしくない状況にある。また、グローバルなサプライチェーン等におけるひとつの点への攻撃が他の拠点へも影響することが危惧される。

サイバー攻撃はその手法の入手が容易であり、国家のみならず多様な主体が隠蔽や偽装等を行うことに加え、世界中から実行することが可能である。サイバー攻撃は、我が国に直接行われることもあれば、他国に係るサイバー空間を経由して行われたり、我が国に係るサイバー空間を踏み台にして行われたりすることもあり得る状況となっている。また、サイバー攻撃と武力攻撃等の関係については国際的に定説がない状況であるが、武力攻撃等に該当するサイバー攻撃がこのような形で行われる可能性も否定できない状況となっている。

(2)これまでの取組

我が国においては、情報セキュリティ政策に係る司令塔として、基本戦略の立案その他官民における統一的・横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行うため、2005年4月、内閣官房に情報セキュリティセンター(National Information Security Center。以下「NISC」という。)[32]が設置された。また、同年5月には、官民における統一的・横断的な情報セキュリティ対策の推進を図るため、高度情報通信ネットワーク社会推進戦略本部に情報セキュリティ政策会議(以下「政策会議」という。)[33]が設置され、政

ードディスクの内容が消去される可能性があります。韓国での被害発生と同時期に、日本にも同じ不正プログラムが少なからず流通していたと推測されます。」と発表されている。

30 遠隔操作ウイルス「iesys.exe」に感染した一般利用者のPCを遠隔操作することにより、当該一般利用者に成りすまして、インターネット掲示板等への大量殺人等の予告等が行われた事案。本事案においては、高度匿名化技術の1つであるTor(The Onion Router)が悪用された。

31 例えば、米国におけるトレードシークレット(営業秘密)の窃取の抑制に関する戦略であるAdministration Strategy on Mitigating the Theft of U.S. Trade Secrets(White House, Feb. 2013)や国防総省による年次報告書であるAnnual Report to Congress (Department of Defence, May 2013)。

32 内閣官房組織令(昭和32年政令第219号)第12条に基づく「情報セキュリティセンターの設置に関する規則」(平成12年2月29日内閣総理大臣決定)。

33 高度情報通信ネットワーク社会推進戦略本部令(平成12年政令第555号)第4条の規定に基づく「情報セキュリティ政策会議の設置について」(平成17年5月30日高度情報通信ネットワーク社会推進戦略本部長決定)。

府機関や重要インフラ事業者の情報セキュリティ水準の向上、サイバー攻撃への対処能力の強化等が推進されている。

政策会議においては、これまで、「第1次情報セキュリティ基本計画」[34]（以下「第1次計画」という。）をはじめとして、3次にわたり、包括的な中長期計画としての戦略を策定してきている。

第1次計画においては、情報セキュリティについて、情報通信技術の利活用を通じた経済の持続的発展とより良い国民生活の実現、それにより発生する脅威からの安全保障という国家目標の中に位置づけるとともに、情報セキュリティ問題に対する足元を固める観点から、顕在化した問題への対処療法的な対応から事前対策の取組への転換を推進してきた。また、政府機関、重要インフラ事業者や企業等の各主体について、縦割り構造の中でそれぞれが独自の対応に終始する状態から、自らの責任を自覚しながら、それぞれの立場に応じた適切な役割分担を果たす枠組みを立上げてきた。

「第2次情報セキュリティ基本計画」（以下「第2次計画」という。）[35]では、従来の事前対策の取組を引き続き着実に推進するとともに、万が一の事態においても迅速な対応等を進めることで、事業継続性を確保するという「事故前提社会」における事後対応力の強化が行われてきた。

これらの取組を継続しつつ、「国民を守る情報セキュリティ戦略」（以下「国民を守る戦略」という。）[36]においては、サイバー空間に係る全ての脅威に対する対応力を世界最高水準に高めることを目標とし、海外における大規模サイバー攻撃事態の発生等の環境変化に対応し、その対処体制の整備や平素からの情報収集・共有体制の構築・強化等の安全保障・危機管理の観点からの取組が進められてきている。

このように、第1次計画により情報セキュリティ政策が立上げられて以来、経済の持続的発展や社会的課題の解決のための情報通信技術の利活用環境の構築、「事故前提社会」への対応や安全保障・危機管理の観点からの取組が強化され、新たな環境変化に的確に対応してきており、それぞれの戦略に基づく取組については、概ね計画どおり実現されてきたといえる。

しかしながら、サイバー空間が急速に拡大・浸透し、サイバー空間を取り巻く

[34] 2006年2月2日情報セキュリティ政策会議決定。
[35] 2009年2月3日情報セキュリティ政策会議決定。
[36] 2010年5月11日情報セキュリティ政策会議決定。

リスクの甚大化、拡散及びグローバル化が顕著に進むなど、リスクの深刻化が進展していることから、次元を変えた取組が必要となっている。

(3)国際的な動向

官民など多様な主体が参加する国際会議、国際連合や地域機関等の国際機関などの場[37]において、サイバー空間に関する行動規範、サイバー空間を利用した行為に対する国際法の適用やインターネットガバナンス等のサイバー空間の在り方に関する議論が活発に行われている。

諸外国においても、サイバー空間を取り巻くリスクに対応するため、国家安全保障や経済成長等の観点から、「サイバーセキュリティ」[38]に関する国家戦略が策定されている。サイバー空間の在り方については、もはや世界的に共通の課題となっており、グローバルな視点による取組が必要となっている。

【米国】

米国においては、サイバーセキュリティが国家として直面する最も深刻な経済的かつ国家安全保障上の課題とされており[39]、「国家安全保障戦略」[40]においても、サイバーセキュリティに関する脅威が国家安全保障、公共の安全及び経済発展にとっての最も深刻な挑戦と位置付けられている。これらを踏まえ、2011年には、個別分野に関する戦略が策定されている。

例えば、国際貿易等を支え、国際安全保障を強化し、表現の自由とイノベーションを促進し、オープンで、相互運用性があり、セキュアかつ信頼できるサ

---

[37] 例えば、APEC（アジア太平洋経済協力）電気通信・情報産業大臣会合（2010年10月沖縄）、OECD（経済協力開発機構）インターネット経済に関するハイレベル会合（2011年6月パリ）、APT（アジア・太平洋電気通信共同体）サイバーセキュリティフォーラム（2011年12月東京）、サイバー空間に関する国際会議（2011年11月ロンドン、2012年10月ブダペスト）、ITU（国際電気通信連合）世界国際電気通信会議（WCIT。2012年12月ドバイ）、NATO（北大西洋条約機構）CCD COE（サイバー防衛センター）や国連総会第一委員会（国際安全保障・軍縮担当）の「国際安全保障の文脈における情報及び電気通信分野の進歩」に関する政府専門家グループ（2012年～）がある。

[38]「サイバーセキュリティ」の定義には各国共通の理解がないのが現状である。例えば、欧州ネットワーク情報セキュリティ庁（ENISA）の「National Cyber Security Strategies – Practical Guide on Development and Execution」（Dec. 2012）において、「EUレベルにおいても、国際レベルにおいても、サイバーセキュリティの統一的な定義が欠けている」とされている。

[39] The Comprehensive National Cybersecurity Initiative (White House, Jan. 2008)、The Cyberspace Policy Review (White House, 2009)。

[40] National Security Strategy (White House, May 2010)。

イバー空間を国際的に発展させるという将来像を示した「サイバー空間の国際戦略」[41]、インターネットビジネス分野におけるイノベーションを阻害せず、多大な経済的・社会的価値を守るための戦略[42]、陸・海・空・宇宙にサイバー空間を新たに加える等の「サイバー空間における作戦のための国防総省戦略」[43]、セキュアで強靭なインフラを支え、イノベーションと繁栄をもたらし、設計段階からプライバシー等市民の自由が保護されるサイバー空間を目指し、重要な情報インフラの保護とサイバーエコシステムの確立を図る「国土安全保障分野のためのサイバーセキュリティ戦略」[44]が策定されている。

【EU】

EUにおいては、自然災害やテロ等に加え、経済スパイや国家支援によるサイバー攻撃という国境を越えた新たな脅威により、サイバーセキュリティインシデントの頻度・規模が増大し、ヘルスケア、電力や自動車等の重要サービスの供給が破壊されるなど国家の安全や経済に多大な損害を及ぼし得るという認識の下、2013年2月に、サイバー攻撃等の予防や対応に関する包括的な将来像を示した「EUサイバーセキュリティ戦略」[45]が策定されている。

---

[41] International Strategy for Cyberspace (White House, May 2011)。国内外や官民の連携が必要な活動領域として、①経済、②自らのネットワークの保護、③法執行、④軍、⑤インターネットガバナンス、⑥国際開発、⑦インターネットの自由を優先的な政策として提示している。

[42] Cybersecurity, Innovation and the Internet Economy (The Department of Commerce Internet Policy Task Force, June 2011)。重要な情報インフラとして分類されない、オンラインサービスを提供する中小企業やインターネット上だけの大企業等の「インターネット・情報イノベーション分野」を対象とし、①ガイドライン作成等による脆弱性最小化のための国家的アプローチの創出、②インシデント報告や情報共有等に関するインセンティブ構築、③教育及び研究開発、④国際標準化やベストプラクティスの共有等の国際連携が提言されている。

[43] Department of Defense Strategy for Operating in Cyberspace (July 2011)。イニシアティブとして、①サイバー空間を作戦領域の１つに位置付け、優先的に作戦を策定等できる体制構築、②国防総省の情報ネットワーク保護のための新戦略の策定、③他機関や民間企業との連携推進、④同盟国との連携強化及び国際的パートナーシップの構築、⑤人材育成及び革新的な技術開発の推進が示されている。

[44] Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise (Department of Homeland Security, Nov. 2011)。重要な情報インフラの保護について、①重要な情報インフラの特定、技術革新等によるリスク削減、②緊急事態への準備等による優先対応等の確保、③情報分析・共有、専門的訓練の提供等の人材育成等による状況認識の共有、④システム障害への耐性強化を目的とし、サイバーエコシステムの確立については、①官民の人材育成、普及啓発等によるリテラシー向上、②脆弱性の削減、利便性の向上による製品等の信頼性向上、③機器間の相互運用性の向上、セキュリティプロセスの自動化等による連携体制の構築、④公衆衛生に関する情報共有と同様のセキュリティに関する情報共有、認証機器等の情報共有、インセンティブ付与等による透明性の確保を目的としている。

[45] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, Feb. 7, 2013)。優先事項として①サイバーレジリエンスの実現、②サイバー犯罪の劇的削減、③共通安全保障防衛政策に関するサイバー防衛政策・能力の開発、④サイバーセキュリティの産業・技術開発、⑤包括的な国際戦略の策定と中核となる価値観の促進を掲げている。

本戦略においては、サイバー空間がオープンで自由であるために、基本的人権、民主主義及び法の支配という基本原則や価値観が、オフラインと同様に適用されるべきとするとともに、インシデントや悪意ある活動等から保護するなど政府が重要な役割を果たすとされている。

【イギリス】

イギリスにおいては、インターネットによる成長促進等と同時に、重要なデータやシステムのサイバー空間への依存が高まることにより、検知や防御が困難な新たなリスクがもたらされているという認識の下、2010年に、サイバー攻撃を最優先の脅威とする「国家安全保障戦略」[46]が策定されている。

サイバー攻撃の脅威に対応するにあたって、2011年には、活発で、レジリエントかつセキュアなサイバー空間から多大な経済・社会的価値を引き出し、自由、公正、透明性及び法の支配という中核的な価値の下で、繁栄、国家安全保障及び強い社会を促進するという将来像を示した「サイバーセキュリティ戦略」[47]が策定されている。

【フランス】

フランスにおいては、2008年に発表された国家安全保障に関する戦略となる「防衛と国家安全保障に関する白書」[48]により、新たな脆弱性として、サイバーセキュリティが主要なテーマとして扱われている。

2011年には、この国家安全保障戦略を踏まえ、世界的なサイバーディフェンス大国になること、国家主権に関する情報の保護により国家の意思決定能力を守ること、国家の重要インフラのサイバーセキュリティを強化すること、サイバー空間における情報セキュリティを確保することを目的とする「情報システム

---

[46] A Strong Britain in an Age of Uncertainty: The National Security Strategy (Cabinet Office, Oct. 2010)。

[47] The UK Cyber Security Strategy Protecting and promoting the UK in a digital world (Cabinet Office, Nov. 2011)。目標として、①サイバー犯罪対策等により、サイバー空間でビジネスを行う上で、世界で最も安全な場所の１つになること、②サイバー空間の防衛力強化や脅威の検知能力の向上等によるサイバー攻撃からの国家インフラの防御等を通じ、サイバー攻撃に対するレジリエンスを向上させること、③オープンで相互運用可能なサイバー空間の促進等により、セキュアに利用でき、オープンで、安定的、活発なサイバー空間の構築を支援すること、④横断的な研究開発、脅威、脆弱性やリスクの理解の深化、インシデント対応能力の強化等により、サイバーセキュリティに必要な分野横断的な知識、技術、能力を備えることを掲げている。

[48] The French White Paper on Defense and National Security (Conseil d'État, 2008)。

保護・セキュリティ戦略」[49]が策定されている。

【ドイツ】

ドイツにおいては、サイバー空間の利用可能性とそれにおけるデータの完全性や機密性等が21世紀における最重要課題であり、サイバーセキュリティの確保が、国内的にも国際的なレベルにおいても、国家、企業、社会が共有すべき共通課題であるとの認識の下、2011年2月に、経済・社会的繁栄を維持・促進することを目的とする「サイバーセキュリティ戦略」[50]が策定されている。

【韓国】

韓国においては、サイバー攻撃が国民の財産や国家安全保障を脅かす状況にまで至っているという認識の下、ますます高度化しインテリジェントになっている国家レベルのサイバー脅威に対応するための体制を整備し、関係する行政機関の役割の明確化を図る等によりサイバー空間を守るため、2011年8月に、「国家サイバーセキュリティマスタープラン」が策定されている[51]。

---

[49] Information systems defense and security – France's strategy (ANSSI, Feb. 2011)。取組領域として、①適切な判断を行うための分析と予測、②攻撃の検知、潜在的な被害者への注意喚起及びサポート、③科学技術、産業、人的能力の強化等による独立性の確保、④国家の情報システム及び重要インフラの保護によるレジリエンスの確保、⑤技術開発新たなプラクティスに適応した法制度、⑥情報システムセキュリティ、サイバーディフェンス、サイバー犯罪対策における国際連携による情報システムの保護、⑦国民の理解向上のための情報提供及び啓蒙活動を掲げている。

[50] The Cyber Security Strategy for Germany (Federal Ministry of the Interior, Feb. 2011)。重要分野として、①重要な情報インフラの保護、②国内における安全なITシステム、③行政機関におけるITセキュリティの強化、④国家サイバーレスポンスセンター、⑤国家サイバーセキュリティ評議会、⑥サイバー空間における効果的な犯罪の抑制、⑦欧州及び世界規模におけるサイバーセキュリティの確保のための効果的な連携、⑧信頼できる情報技術の活用、⑨連邦政府における人材育成、⑩サイバー攻撃に対応するためのツールを掲げている。

[51] National Cyber Security Masterplan – Protecting national cyber space from cyber attacks (National Cyber Security Center, Aug. 2011)。重点的な推進課題として、①脅威の早期検知及び対応体制の整備、②重要な情報とインフラのセキュリティの強化、③サイバーセキュリティの一層の強化のための基盤整備、④サイバーにおける挑発の抑止と国際協調の強化、⑤重要な情報とインフラのセキュリティマネジメントレベルの向上を掲げている。

2. 基本的な方針

(1)目指すべき社会像

サイバー空間がグローバルに繋がる中、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のためには、サイバー空間を取り巻くリスクの深刻化への対応及び実空間との融合・一体化の進展との両立を図り、サイバー空間の持続性・発展性を確保することが重要になっている。

このため、我が国においては、「世界を率先する」「強靱で」「活力ある」サイバー空間を構築し、これが社会システムとして組み込まれることにより、サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会として、「サイバーセキュリティ立国」を実現することを目指す。

(2)基本的な考え方

サイバーセキュリティ立国を実現するにあたり、我が国における基本的な考え方は次のとおりである。

①情報の自由な流通の確保

我が国においては、管理や規制を過度に行うことなく、開放性や相互運用性を確保することにより、情報の自由な流通が確保された安全で信頼できるサイバー空間の構築に努めてきた。

その結果、サイバー空間において、表現の自由、プライバシーの保護等が確保されるとともに、イノベーション、経済成長、社会的課題の解決などの様々な恩恵を我が国にもたらしてきている。

本戦略においても、このような情報の自由な流通の確保を基本的な考え方として、我が国におけるサイバー空間を取り巻くリスクの深刻化に対応していくことが必要である。

②深刻化するリスクへの新たな対応

サイバー空間を取り巻くリスクは深刻化しており、早急な対応が必要となっている。とりわけ顕著に進行している、甚大化するリスク、拡散するリスク、さらに、グローバルリスクについては、これまでの戦略で講じてきた様々な取組の延長では十分に対応できなくなっている。

サイバー空間がサイバー攻撃等に対して脆弱であった場合には、情報の自由な流通を確保することが困難になるとともに、サイバー空間に対する国民の信頼も確保できなくなると考えられる。

このため、これまでの事前・事後対策や対処体制の整備等による個別対応の取組に加え、情報通信技術の革新等に伴うリスクの変化に迅速かつ的確に対応できる社会システムとして、多層的な取組による新たなメカニズムが必要である。

③リスクベースによる対応の強化

我が国においては、これまで、サイバー空間を取り巻く全ての脅威に対する対応力を世界最高水準に高めることを目標[52]とし、政府機関、重要インフラ事業者等、企業及び個人など各主体が、それぞれの情報セキュリティ対策に最大限の努力で取り組むという方針で進めてきた。

しかしながら、守るべき重要な情報や情報システムのサイバー空間への依存が一層高まる中、手法の複雑・巧妙化等によりサイバー攻撃の脅威も高まっている。このような状況では、各主体によるこれまでの取組は継続しつつも、刻々と変化するリスクに対し、社会メカニズムとして、適時適切な資源配分の下で動的に対応していくこと[53]が必要である。

サイバー攻撃に関するインシデントの認知・解析機能の向上、これらの機能の連携、情報共有の促進による脅威分析能力の高度化、各主体のCSIRT[54]

---

[52] 国民を守る戦略では、「実現すべき成果目標」として、「サイバー攻撃等、情報通信技術に係る全ての脅威に対する対応力を世界最高水準に高める」こととされている。

[53] 例えば、Observe（モニタリング）、Orient（情勢判断）、Decide（意思決定）、Act（行動）を繰り返すことにより、迅速かつ適格な意思決定を行う「動的防御プロセス連携」（OODA ループ）。「総務省における情報セキュリティ政策の推進に関する提言」（平成 25 年 4 月 5 日情報セキュリティアドバイザリーボード）参照。

[54] Computer Security Incident Response Team。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。

間の連携や国際的なCSIRT間連携[55]の強化等が重要であり、これらによる動的対応力を通じ、リスクの性質を踏まえたリスクベースによる対応を強化することが必要である。

④社会的責務を踏まえた行動と共助

我が国においては、実空間におけるあらゆる活動がサイバー空間に依存しており、官・公・学・産・民に渡る多種多様な主体が、その恩恵を享受している。

従って、サイバー空間を取り巻くリスクが深刻化する中、それぞれの主体においては、世界を率先する強靭で活力あるサイバー空間を実現するという社会的責務の下で、自ら情報セキュリティ対策を行うなど主体的に行動していくことが必要である。

その上で、リスクが拡散している状況にあっては、サイバー空間を介し広く被害が波及することから、個々の主体による対策に加え、不正な侵入やマルウェア感染等に対して、社会全体が参加することで予防的に情報セキュリティ対策に取り組む「サイバー空間の衛生」が重要になっている。

このため、サイバー空間におけるマルチステークホルダーがそれぞれの社会的立場に応じた役割を発揮しながら、国際連携や官民連携をはじめとして相互に連携し、共助することが必要になっている。

(3)各主体の役割

これまでの戦略においては、それぞれの主体が自らの責任を自覚しながら、その立場に応じた適切な役割分担の下で対策を実施することとしている。具体的には、情報セキュリティ対策を実際に適用し、実施する「対策実施主体」と、その対策の手法や環境整備を側面的に支援し、問題の理解・解決を促進する「対策支援主体」について、それぞれ期待される役割と連携の在り方[56]を提示

[55] (一社) JPCERT コーディネーションセンター (Japan Computer Emergency Response Team Coordination Center。以下「JPCERT/CC」。) により、国内に加えて国際的な CSIRT 間連携が図られ、インシデント対応が進められている。

[56] 第１次計画以降、「新しい官民連携モデル」として、具体的には、①「政府機関・地方公共団体」、②「重要インフラ」、③「企業」及び④「個人」という「対策実施主体」と、①政策を立案・実施する主体としての「政府・地方公共団体」、②初等中等教育機関、高等教育機関及び研究開発・技術開発実施機関である「教育・研究機関」、③情報システムの構築や通信サービスの提供等 IT 基盤を構築・提供している事業者である「情報関連事業者」等及び④「メディア」という「対策支援主体」からなる枠組みが構築されてきた。

し、情報セキュリティ対策が推進されてきた。

また、以上の主体に加え、第2次計画以降においては、「事故前提社会」への対応力を強化するとともに、国民や社会が、情報セキュリティに関する絶対的な無謬性の追求から脱却し、自ら主体的に考える力強い「個」と「社会」を確立する観点から、自己の情報等を預ける「情報提供主体」及びそれを預かる「情報管理主体」も視野に入れた取組[57]が推進されている。

本戦略においては、サイバー空間と実空間の融合・一体化が進展し、サイバー空間を取り巻くリスクが深刻化するという新たな局面を踏まえ、これまでの各主体における縦割り構造を前提とした枠組みから脱却し、サイバー空間に依存する各主体が対策実施主体であると同時に、対策支援主体であるという観点から、各主体の役割を示すこととする。

サイバー空間に依存する多種多様な主体が、それぞれの役割を発揮しつつ、相互に連携しながら共助することにより、社会全体による動的対応力を強化していくことが必要である。

①国の役割

国は、サイバー空間に関する国家の基本的な機能を強化することが必要である。具体的には、国際的な規範形成への積極的な参画等のサイバー空間に関する外交をはじめとして、外国政府等が関与するサイバー攻撃等から我が国に係るサイバー空間を守る「サイバー空間の防衛」や、サイバー空間の犯罪対策に取り組むことが必要である。

また、自ら重要な情報を保有し情報システムを運用する、電子行政の推進と密接な関連により情報セキュリティ対策を実施する主体として、政府機関及びそれと密接な関係にある独立行政法人や特殊法人等における対策の強化に取り組むとともに、その取組によって他の主体における取組を先導することが求められる。同時に、サイバー攻撃発生時の対処態勢を充実・強化し、政府機関等に対してサイバー攻撃がなされた場合の被害の極小化を図ることが必要である。

[57] 第２次計画では、「情報提供主体」について、「潜在的にそうなり得る者も実際に情報を預けている者も双方含む」ものであり、「全ての主体が情報提供主体となり得る」とされている。また、「情報管理主体」については、「実質的には、対策実施主体と同じ範囲を指す」とされている。

さらに、政府機関自らも含め、他の主体がその役割を最大限に発揮できるようにするため、国は、司令塔としてのNISCの機能強化を図り、関係省庁間を含む各主体間の連携を促進するとともに、新たな制度整備、先端的な技術開発、実証実験、高度な人材の育成やリテラシーの向上等を積極的に行うことが必要である。

②重要インフラ事業者等の役割

他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤である「重要インフラ」[58]については、これがサイバー攻撃等により機能障害を起こした場合、国民生活等に甚大な被害をもたらす可能性がある。

このため、我が国においては、現在、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道及び物流の10分野に属する「重要インフラ事業者等」に対し、情報セキュリティ確保において政府機関等における対策に準じた取組を求めている。これら事業者等においては、今後も更に取組強化を行っていくことが必要である。

また、我が国においてはこれまで重要インフラと位置付けられてこなかったが、当該サービス等に係る情報システムの障害等が国民生活及び社会経済活動に多大な影響を及ぶす恐れのある分野が存在する。具体的には、スマートシティやスマートタウン、ITS等の交通制御システム等の新たなネットワーク系サービスや、米国で重要インフラに含まれている防衛産業、エネルギー関連産業等[59]である。

今後、政府において、これらの重要インフラと位置付けられていない分野における情報システムの位置づけを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について検討することとし、重要インフラの範囲等の見直しが行われた場合、新たに重要インフラ事業者等となる者において

---

58 「重要インフラの情報セキュリティ対策に係る第２次行動計画」（2009年２月３日情報セキュリティ政策会議決定、2012年４月26日改定）においては、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの」とされている。

59 Critical Infrastructure Protection Act of 2001において、米国にとって非常に重要な物理的又は仮想的なシステムや資産であり、それらの無力化や破壊により、セキュリティ、国家の経済安全保障、国民の公衆衛生や安全、又はそれらの組み合わせを衰えさせるような影響を与えるものとして、18の分野が対象となっている。

は、必要な対策を行っていくことが求められる。

③企業や教育・研究機関の役割

企業や教育・研究機関は、技術情報、財務情報、製造技術や図面等の知的財産関連情報、顧客名簿、人事情報や学習指導情報等の個人情報などを保有している。

我が国産業の国際的な競争力の源としても重要な情報が、サイバー攻撃等により窃取や破壊等された場合、我が国の社会経済発展を阻害する可能性がある。従って、企業や教育・研究機関においては、個々における情報セキュリティ対策に加え、サイバー攻撃に関する情報共有など業界団体等による集団的な対策に取り組むことが期待される。なお、各々の主体において情報セキュリティ対策に取り組む際には、必要に応じて、第三者専門機関から、評価、監査を受けて、マネジメント標準を取得する等により、対策を向上していくことが期待される。

また、技術開発と人材育成の中核になる主体として、企業や教育・研究機関は、産官学連携の下、それぞれが協調し、我が国において、世界を率先する強靭で活力あるサイバー空間を構成する高度な技術や人材等を供給することが期待される。

④一般利用者や中小企業の役割

一般利用者や、我が国企業のほとんどを占め[60]サプライチェーンの中核となっている中小企業においては、利便性の向上、業務の効率化やサービス提供の迅速化等の観点から、情報通信技術による新たなサービスが日々活用されている。

全人口の約8割がインターネット利用者となり[61]、企業のインターネット利用率がほぼ100%となる[62]など情報セキュリティ対策が必要となる対象が非常に

[60] 総務省「平成21年経済センサス－基礎調査」によると、中小企業数（会社数及び個人事業者数）は、約420.1万社であり、全企業数に占める割合は99.7%、また、中小企業の会社数は約177.5万社で、全会社数に占める割合は99.3%。
[61] 通信利用動向調査によると、平成23年にインターネットを利用したことのある人は推計で9,610万人となり、人口普及率は79.1%。
[62] 通信利用動向調査によると、平成23年末において、企業のインターネット利用率は98.8%。

広範囲に及んでいる中、一般利用者等が使用するスマートフォン等がセキュリティホールとなり、サイバー攻撃の対象となる場合には、サイバー空間を介し、他の主体にも被害が波及する可能性がある。

これまでも一般利用者等においては、自助努力による対策が行われてきたところである。今後は、一般利用者等が「自分の身は自分で守る」[63]とともに、「他者に迷惑をかけない」[64]という認識をもって対策に取り組むことが重要となっている。従って、一般利用者等においては、各主体の活動も活用しつつ、この認識の醸成やリテラシーの向上等により、自律的に取り組むことが期待される。

また、中小企業のうち、重要インフラ事業者や先端的な技術を有する事業者等と契約関係にあることなどにより我が国の重要な情報やシステムを取り扱っている事業者については、個々における情報セキュリティ対策に加え、サイバー攻撃に関する情報共有等の取組が期待される。

⑤サイバー空間関連事業者の役割

サイバー空間については、それを構成する機器、ネットワークやアプリケーション等が、端末製造事業者、インターネットアクセス提供事業者、ネットワーク管理事業者やソフトウェア開発事業者等の民間企業を中心として提供されている。また、サイバー空間を取り巻くリスクに対応するためのツールについても、民間企業が中心となって提供されている。

これまでの戦略においても、各主体が情報セキュリティ対策を行うにあたっての直接的なツールを実際に提供する「情報関連事業者」については、その提供する製品やサービスにおける脆弱性を極力排除する責任を負うとともに、国際競争力の向上も見据え、より安全・安心な製品等を提供するよう努める観点から、重要な主体として位置づけられてきている[65]。

---

[63] 第１次計画において、対策実施主体としての個人の役割として、「『知らない人に付いていかない』といった極めて一般的な安全に対する認識と同等の認識を情報セキュリティに対しても、醸成していくことが必要である。自分の身は自分で守るという原点を明確に認識して行動することが期待される」とされている。

[64] 2012 年９月 28 日、情報セキュリティ国際キャンペーンの実施に当たっての官房長官メッセージにおいて、「情報セキュリティ対策を怠ると自らに害が及ぶだけでなく、知らないうちに他の人に害を与えてしまいます。情報セキュリティ対策をしっかり行い、安全に、安心してスマートフォンやパソコンを利用するようにして下さい。」とされている。

[65] 第１次計画において、「情報関連事業者は、政府機関・地方公共団体、重要インフラ、企業、個人のそれぞれが対策を実施するにあたり、直接的なサービスを実際に提供する主体であり、我が国の情報セキュリティの基盤強化を支える役割を担う。したがって、それぞれが提供する製品・サービスにおける脆弱性を極力排除する責任を負うという点を改めて認識し、より安全・安心な

しかしながら、製品等におけるソフトウェアの脆弱性は、開発段階で全て排除しきることは困難であるとともに、一般利用者等の各主体における対策のみでは、多様な主体が依存するサイバー空間を介したリスクの拡散に対し、隅々まで対応することが困難となっている。

従って、サイバー空間に係る製品、サービスや技術等を提供する「サイバー空間関連事業者」においては、開発時にそれらにおける脆弱性を作りこまないように努めるとともに、開発後に脆弱性が発見された時点で適切な対策をとるなどによる脆弱性の排除や、サイバー攻撃に関するインシデントの認知・解析等を通じて、被害の拡大を防止するなどサイバー空間の衛生の確保に取り組むことが期待される。

また、現在、情報セキュリティ対策に関する製品等を海外事業者に大きく依存し、国内におけるセキュリティ従事者も不足する中、サイバー空間関連事業者においては、高度な技術や製品の開発やそれらの情報セキュリティ対策での利活用による市場創出等により、我が国の「サイバーセキュリティ産業」の国際競争力を強化することが重要である。

3. 取組分野

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ため、政府は、これまでの「事故前提社会」に対応した取組を継続するとともに、国内における他の主体及び関係諸国等と共助しつつ、2015年度までの3年間、以下に掲げる取組を進めることとする。

以下の取組を進めるにあたっての具体的な目標として、2015年度までに、政府機関及び重要インフラ分野におけるサイバー攻撃に関する情報共有体制のカバー率の向上、CSIRT設置率の向上、マルウェア感染率[66]や国民の不安感[67]の改善を目指すとともに、国際的なインシデント調整の対応連携が可能

製品・サービスを提供するよう努める必要がある。なお、その際には、安全・安心なサービスの提供が、最終的には、その情報関連事業者の国際的競争力の向上にも繋がるというプラスの視点を持つことも重要である。」とされている。

[66] 例えば、マイクロソフト「セキュリティインテリジェンスレポート」において、CMM（Computers Cleaned per Mille。悪意あるソフトウェア削除ツール 1,000 回実行あたりにマルウェア及び望ましくない可能性のあるソフトウェアがクリーニングされたパソコンの台数を示したもの。）という指標を用いて世界各国の状況の比較を行っている。我が国の感染率は 2012 年 1 年間を通して 1 以下（0.7～0.9）とされている。

[67] 例えば、情報通信白書では、インターネット利用で感じる不安等について、平成 23 年には、世帯について「ウイルスの感染が心配である」が 72.8%、企業について「ウイルス感染に不安」が 41.4%となり、それぞれ最も高いものとされている。

な国[68]やサイバー攻撃対応に関する国際的な連携や対話の相手国等の数の3割増を目指すものとする。また、2020年までの目標として、国内の情報セキュリティ市場規模[69]の倍増やセキュリティ人材の不足割合の半減を目指すものとする。

なお、以下の取組にあたっては、サイバーセキュリティが世界的に共通の課題となっていることから、サイバー攻撃事案やサイバーセキュリティに関する政策等の海外動向について調査・分析するとともに、諸外国等とも情報交換など連携しながら進めることが必要である。

政府は、「政府機関の情報セキュリティ対策のための統一基準群」[70]、「重要インフラの情報セキュリティ対策に係る第2次行動計画」（以下「第2次行動計画」という。）[71]、「情報セキュリティ研究開発戦略」[72]、「情報セキュリティ人材育成プログラム」[73]及び「情報セキュリティ普及啓発プログラム」[74]等を見直し、必要に応じて新たな計画等を策定する。

（1）「強靭な」サイバー空間の構築

サイバー空間の持続性を確保するため、サイバー攻撃への対応を増強するとともに、サイバー攻撃に関するインシデントの認知・解析やインシデント等関連情報の共有等の機能を高めること等により、「強靭な」サイバー空間を構築し、サイバー攻撃等に対する防御力・回復力の強化を目指す。

①政府機関等における対策

---

[68] 例えば、現在、JPCERT/CC では、窓口 CSIRT 間でのインシデント調整において対応連携が直接できる国は、80 か国程度となっている。

[69] 例えば、現状において、我が国の情報セキュリティ市場（製品及びサービス）の規模は、5,853 百万ドル（2010 年）であり、米国に次ぎ世界第 2 位にあり、我が国 GDP に占める割合は 0.107%（2010 年）であり、英国、米国に次ぐ水準にある。また、同市場の構造について、我が国においては製品（1,428 百万ドル）よりもサービス（4,425 百万ドル）の市場が大きくなっている。経済産業省「情報セキュリティの市場調査」。

[70] 「政府機関の情報セキュリティ対策のための統一規範」（2011 年 4 月 21 日情報セキュリティ政策会議決定、2012 年 4 月 26 日改定）及び「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」（2005 年 9 月 15 日同会議決定、2012 年 4 月 26 日改定等）など。

[71] 2009 年 2 月 3 日情報セキュリティ政策会議決定、2012 年 4 月 26 日改定。

[72] 2011 年 7 月 8 日情報セキュリティ政策会議決定。

[73] 2011 年 7 月 8 日情報セキュリティ政策会議決定。

[74] 2011 年 7 月 8 日情報セキュリティ政策会議決定。

政府機関等においては、その情報及び情報システムに係る情報セキュリティ水準の一層の向上を図るとともに、サイバー攻撃への対処態勢を充実・強化する。

【情報及び情報システムに係る情報セキュリティ水準の一層の向上】

政府機関において、国家機密等に関する情報及び情報システムの重要度等に応じた情報セキュリティ対策の重点化を行うため、標的型攻撃等への対処に関するリスク評価手法の確立等を通じて、政府機関における統一的な仕組みを強化する。また、規律をもちつつ、テレワークやBYODなど多様化する国家公務員の就労形態に対応した適切な情報セキュリティの確保を図るための環境整備を行う。加えて、SNSの利用については、重要な情報を国民に提供するに際し、我が国が責任と規律をもって行うことができることを前提とする。

政府横断的な情報システムの対策強化に取り組む。具体的には、政府共通プラットフォーム[75]による政府情報システムのクラウド化等を通じて、サイバー攻撃や大規模災害に強い政府情報システム基盤を構築する。また、社会保障・税番号制度について、政府機関や地方自治体等が管理・運用する情報提供ネットワークシステム等[76]における情報セキュリティ対策の強化を図る。加えて、電子行政オープンデータの推進[77]においても情報セキュリティの確保に取り組む。

政府機関の情報システムについて、その設計、製造、設置等の段階において情報セキュリティの技術標準化やその適合性の評価結果の活用が必要であり、さらに、既知脆弱性への未対応、危殆化された技術の利用やマルウェアを埋め込まれる等のサプライチェーン・リスクへの対応強化が必要である。具体的には、国際規格に基づく適合性評価制度[78]の活用や、政府調達に関する協定における国家安全保障のための必要な措置[79]の適用など政府調達の在り方について国際約束において認められる範囲内で検討する。暗号技術について

---

[75] 2013年3月から運用開始。
[76] 2013年3月1日、「行政手続における特定の個人を識別するための番号の利用等に関する法律案」（番号法案）を国会に提出。
[77] 「電子行政オープンデータ戦略」（平成24年7月4日IT戦略本部決定）。
[78] 国際貿易におけるITセキュリティの評価及び認証のスキームとしては、例えば、CCRA（Common Criteria Recognition Agreement）がある。
[79] WTO政府調達協定（Agreement on Government Procurement。1995年1月に発効したWTO協定の附属書四に含まれる複数国間貿易協定の1つであり、別箇に受諾を行ったWTO加盟国のみが拘束。）第23条において、国家の安全保障上の重大な利益を保護する場合等に関する適用除外が規定されている。

は、安全評価がなされたもの[80]の利用を推進する。また、電子政府の推進と緊密に連携を図りながら情報セキュリティ対策を進めていく。

国の安全に関する重要な情報について、国以外の事業者による取扱いにおける情報セキュリティを強化する。こうした情報については、情報処理業務の外部委託、一般の調達及び補助事業等の場合における情報セキュリティ要件の担保が図られている[81]が、これに加え、サイバー攻撃に関するインシデント情報の発注省庁等への報告及び事業者間の情報共有の促進を図る。また、上記の政府機関におけるリスク評価手法の運用にも活用できる枠組みを構築する。

独立行政法人や特殊法人等の国と密接な関係のある法人についても、政府機関における取組に準じて、サプライチェーン・リスクに対するセキュリティの強化を図るとともに、サイバー攻撃に関するインシデントの認知機能を強化し、被害の拡大防止を図る観点から、インシデント情報の法人所管省庁への報告、法人の自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有等を推進する。

【サイバー攻撃への対処態勢の充実・強化】

政府機関等におけるサイバー攻撃認知・解析能力等の大幅向上を図るとともに、インシデント発生時の対処態勢を充実・強化する。

具体的には、GSOC[82]を抜本的に強化することとし、監視対象を一層拡大するとともに、監視対象先におけるインシデント情報の効果的な収集及び高度な解析を可能とするための技術や組織体制等を整備し、あわせて攻撃手法の分析結果等をリスク評価手法の強化に反映させる体制等を整備する。また、収集したインシデント情報や攻撃手法の分析結果等について、監視対象先となる省庁等の政府機関や、重要インフラ事業者等の関係機関と共有するための仕組みも整備する。

---

[80] 総務省及び経済産業省において、電子政府で利用される暗号技術の評価を行い、2013 年 3 月に、「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC（Cryptography Research and Evaluation Committees）暗号リスト）を策定。

[81] 情報セキュリティ政策会議に設置されている情報セキュリティ対策推進会議（CISO 等連絡会議）に設置された「官民連携の強化のための分科会」の検討結果を踏まえ、2012 年 1 月 24 日、「調達における情報セキュリティ要件の記載について」が各省等に対して発出。

[82] Government Security Operation Coordination team（政府機関・情報セキュリティ横断監視・即応調整チーム）。外部からのサイバー攻撃等の情報セキュリティ問題に対して、政府機関の緊急対応能力強化を図るために整備され、2008 年 4 月より運用開始。

インシデント発生時におけるGSOC、CYMAT[83]と各府省庁等のCSIRTの間の連携を強化し、インシデント情報の速やかな共有と政府一体となった即応体制を構築する。また、これまで我が国では、大規模サイバー攻撃事態等[84]を想定して、初動対処訓練の実施など事案発生時の対処態勢を構築する[85]とともに、平素及び事案発生時の情報収集・集約体制の強化を図ってきている。今後も、関係府省庁等が参加した大規模サイバー攻撃事態等対処訓練を毎年度実施するなど対処態勢を強化する。

政府における平常時及び緊急時の対応力を強化するとともに、国際連携を促進するため、人材の確保・育成に取り組むことが必要である。具体的には、優秀な外部人材等の積極的な採用、官民や省庁間の人事交流の促進及び人事ローテーション上の工夫を通じた能力の継続的な開発向上を図る。また、迅速かつ的確な対処を行うため、各府省等のCSIRT要員及びCYMAT要員の育成等を強化する。

我が国に対する情報収集活動が活発に行われる中、最近では、行政機関等に対する情報窃取を目的とした標的型メール攻撃の手法が、複雑・巧妙化し、行政機関の重要な情報が漏えいするリスクがますます高まっていることから、各行政機関が緊密に連携してサイバー空間におけるカウンターインテリジェンスに関する情報の収集・分析・共有に係る取組を一層推進するとともに、外国機関との連携を強化するなどして、より強固な情報保全体制を構築する。

②重要インフラ事業者等における対策

重要インフラ分野については、国民生活、社会経済活動や行政活動等のあらゆる活動が安定的に続けられるようにすることが必要であり、防護対象となる情報システム等の特性に応じ、政府機関等に準じた情報セキュリティ対策に取り組むことが必要である。

---

[83] CYber incident Mobile Assistant Team（情報セキュリティ緊急支援チーム）。平成24年6月にNISCに置かれたものであり、政府CISOである情報セキュリティセンター長の下、府省庁等に対するサイバー攻撃に対し、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言等を行う。

[84] 国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態をいう。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態をいう。

[85] 「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）、「大規模サイバー攻撃事態等への初動対処について」（平成22年3月19日内閣危機管理監決裁）等に基づくもの。

具体的には、重要インフラについて、重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等[86]の策定・変更状況及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針[87]の中に反映するプロセスを確立する。

障害情報及び攻撃・脅威・脆弱性等に関する情報については、引き続き重要インフラ事業者等及びCEPTOAR[88]との間における情報共有を推進するとともに、業種間での情報共有が難しい標的型攻撃に関する情報については、秘密保持契約に基づく情報共有体制を深化・拡充する[89]。また、重要インフラ事業者等による事業所管省庁への迅速な報告、自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有については、個人情報・秘密情報に配慮した上で促進する。さらに、重要インフラ事業者等、サイバー空間関連事業者及び関係CSIRTの間で、民間組織間の信頼関係を前提に、サイバー演習等の実施を促進しサイバー攻撃に対する連携対応能力の強化を図る。

重要インフラ分野におけるサプライチェーン・リスクへの対応強化を図るとともに、情報セキュリティの評価・認証の導入を進めていくことが重要である。具体的には、重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報等の情報共有等による連携の促進、SCADA等の制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討や、制御系機器・システムの評価・認証機関の設立に向けた取組を進めていく。

我が国において、現在、重要インフラとは位置づけられていないが、現行10分野と同等にその情報システムの障害が国民生活及び社会経済活動に多大な影響を及ぼす恐れのある分野について、今後、当該インフラにおける情報システムの位置づけを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について、検討を行う。

---

86 「安全基準」とは、重要インフラ事業者等が、様々な判断、行為を行うに当たり、基準または参考にするものとして策定された文書類（重要インフラの情報セキュリティ対策に係る第２次行動計画）。

87 「指針」とは、「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」及び同「対策編」並びにその後継となるべき文書。

88 Capability for Engineering of Protection, Technical Operation, Analysis and Response（セプター）。重要インフラ 10 分野における情報共有・分析を行う体制。

89 例えば、重要インフラ事業者の関わる取組としては、IPA と民間組織にて標的型サイバー攻撃対策のために運用されているサイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）がある。

以上を踏まえ、第2次行動計画の見直しを実施した上で、新たな行動計画を策定する。

さらに、これまで我が国では、大規模サイバー攻撃事態等を想定して、初動対処訓練の実施など事案発生時の対処態勢を構築するとともに、平素及び事案発生時の情報収集・集約体制の強化を図ってきている。今後も、大規模サイバー攻撃事態等が発生した際に官民が連携して的確な対応を行うことができる態勢を整備するため、必要に応じて諸外国の事例も参考としつつ、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を毎年度実施するなど対処態勢を強化する。

③企業・研究機関等における対策

我が国の国際的な競争力の源として重要な営業秘密等の企業秘密、知的財産情報や個人情報等の重要な情報を取り扱う企業や教育・研究機関において、サイバー攻撃に関するインシデント等の認知・解析機能を強化し、インシデント情報の共有促進を図る。

情報セキュリティ対策に関する専門的な人材の確保や十分な投資等が困難となっている中小企業等について、サイバー攻撃に関するインシデントの認知機能等を強化するための環境整備を行うことが必要である。具体的には、中小企業に寄り添った情報提供・相談体制の整備、情報セキュリティ投資を促進する税制等のインセンティブの検討、情報セキュリティ向上のための利用しやすいガイドライン・ツールの整備やクラウド技術を活用し、情報セキュリティが確保された共同利用システムへの移行促進等を図る。

中小企業等において認知されたインシデント情報の分析や対策情報等の共有を促進するとともに、サイバー攻撃の防御モデルの検討及び演習用テストベッドを利用した実践的な防御演習について、大企業のみならず中小企業等も対象とすることにより、サイバー攻撃への対応能力等の向上を図る。

企業・研究機関等において、インシデントが発生した際の動的対応能力を向上し、被害拡大を防止する観点から、CSIRTの構築を促進し、CSIRT間の連携対応能力の強化等を図る。

サイバー空間を取り巻くリスクの深刻化により企業における経営の不確実性が高まる中、上場企業におけるサイバー攻撃によるインシデントの可能性等に

ついて、競争条件の公平性等に配慮しつつ、事業等のリスクとして投資家に開示することの可能性を検討する。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討する。

また、教育機関については、初等中等教育等における業務の軽減と効率化及び教育活動の質の改善のため、校務の情報化等により学校教育における情報通信技術の利活用が進められていることから、学校設置者である地方公共団体等におけるサイバー攻撃への対応を含む情報セキュリティの確保が図られるよう、情報セキュリティに関する普及・啓発を推進する。

④サイバー空間の衛生

サイバー空間と実空間の融合・一体化が進んでいる状況においては、サイバー空間に相互依存する各主体が、不正侵入やマルウェア感染等に対して予防的に取り組むことにより、サイバー空間の衛生を確保することが重要になっている。しかしながら、リスクが深刻化する中、一般利用者等の自助努力による取組のみでは対応が困難であり、その取組を補強するため、他の主体による積極的なサポートが必要である。

一般利用者等における認識の醸成を目的とする総合的・集中的な普及啓発については、毎年2月の「情報セキュリティ月間」及び毎年10月の「情報セキュリティ国際キャンペーン」として関連行事等を開催している。今後、政府一体としての取組を行うとともに、その一環としてサイバー空間の衛生の確保を国民運動とするため、例えば、放送大学における「情報コース」[90]等の情報セキュリティの基礎となるソフトウェア教育との連携や、功労者の表彰等を行う「サイバー衛生の日（サイバー・クリーン・デー）」（仮称）の新設など一般利用者等の認識の更なる醸成を図るための取組を行う。

また、日常からの効果的な普及啓発について、ソフトウェア等の脆弱性関連情報の収集や各種インターネット定点観測システムの連携等を推進するとともに、我が国におけるサイバー空間の脆弱度やマルウェア感染度等の全体傾向等の可視化や、一般利用者等への的確な発信等を行う仕組みについて検討する。

[90] 2013年4月より、放送大学教養学部に、ソフトウェア、情報数理、マルチメディア、ヒューマン、情報基盤という5つの領域により、情報処理の技術を学ぶのみならず、情報という視点から様々な問題を解決する術を身につけることを目指した情報コースが開設された。

政府機関やサイバー空間関連事業者等が連携し、サイバー攻撃に関するインシデントの認知・解析機能を向上することにより、サイバー空間全体での攻撃に対する対応能力を向上し、一般利用者等への効果的な注意喚起等を図ることが必要である。具体的には、「サイバー攻撃解析協議会」[91]等の取組を通じ、インシデント情報等の提供者との信頼関係を維持しつつ、各機関の専門能力と収集情報を結集し、高度な解析を行うとともに、個別インシデント対応、一般への注意喚起や中長期的な対策検討や研究開発等に活かすことで、サイバー攻撃に対する対応能力を強化する。

ネットワーク型のボットウイルス感染対策として、ISP[92]の協力を得て実施された官民連携プロジェクトであるCCC[93]では、一般利用者に注意喚起等を行う取組が行われてきた。今後、マルウェアを配布する等の悪性サイト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一般利用者に対する注意喚起等を、ISP等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する。

潜在型のマルウェアの挙動等について、高度かつ迅速に検知するための技術開発等を行うとともに、サイバー攻撃の複雑・巧妙化などサイバー空間を取り巻くリスクの深刻化の状況等を踏まえ、情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について検討する。

情報家電、医療機器、自動車や通信ネットワーク等の社会インフラの構成要素が組込みソフトウェアにより制御される環境において、それらのソフトウェアに障害等が発生すれば、人の生命等を脅かす可能性もある。この状況を踏まえ、国際的な整合性を図りつつ、これらに関するソフトウェアの脆弱性への対応に関する制度の検討を行うとともに、機器等を提供するサイバー空間関連事業者が利用者に対しソフトウェア品質を十分に説明できるよう、ソフトウェア品質の説明力の強化を促進する。

---

91 サイバー攻撃からの防御に必要な高度解析を実施するため、総務省、経済産業省、（独）情報通信研究機構（以下「NICT」。）、IPA、テレコム・アイザック推進会議及び JPCERT/CC から構成。

92 Internet Service Provider。光ファイバー回線等を通じて、顧客である企業や一般利用者のコンピュータをインターネットに接続するインターネット接続事業者。

93 Cyber Clean Center。総務省、経済産業省、Telecom-ISAC Japan、JPCERT/CC 及び IPA の連携の下、平成 18 年度から平成 22 年度まで国の事業として実施。

⑤サイバー空間の犯罪対策

サイバー空間において今後起こり得る様々な事態にも対処できるようにするため、サイバー犯罪対処能力の強化や民間事業者等の知見の活用等を図ることにより、国の治安や安全保障・危機管理に影響を及ぼしかねないサイバー攻撃への対処態勢を強化することが必要である。

具体的には、専門的知識・能力を有する者の採用、効果的な教育・訓練や新技術に関する研究等による捜査力及び解析力の強化のほか、サイバー攻撃分析センター、サイバー攻撃特別捜査隊、不正プログラム解析センターの拡充等による体制の整備や、情報収集・分析用資機材の充実強化、インターネット観測用システムの高機能化等の資機材の整備を行う。

民間事業者等の知見を活用した取組の強化については、日本版NCFTA[94]の創設を始め、新種ウイルスに関するアンチウイルスベンダーとの新たな情報共有枠組みの構築、「サイバーインテリジェンス対策のための不正通信防止協議会」等[95]を活用した民間との協力による情報共有の取組の強化、解析対象となる電子機器等の技術情報の共有に関する協力の強化等による情報共有を促進する。また、サイバーパトロールの強化やスマートフォン用アプリに係る被害防止対策の推進等による官民一体となったサイバー犯罪抑止対策を推進するとともに、民間事業者等への手口分析等の嘱託等による民間の知見の捜査等への活用を図る。

サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログの保存期間、一般利用者としての国民の多様な意見等を勘案した上でサイバー犯罪における捜査への利用

---

[94] National Cyber-Forensics and Training Alliance。FBI、民間企業、学術機関を構成員として米国に設立された非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。

[95] セキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者と情報窃取を企図したとみられるサイバー攻撃に関する情報共有等を行う「サイバーインテリジェンス対策のための不正通信防止協議会」のほか、例えば、サイバーテロに関する警察からの情報提供、民間有識者による講演、参加事業者間の意見交換や情報共有を行うため、全ての都道府県において、重要インフラ事業者等との間で構成される「サイバーテロ対策協議会」が設置されている。また、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行うネットワークとして「サイバーインテリジェンス情報共有ネットワーク」が構築され、ウイルス対策ソフト提供事業者等との間で不正プログラム対策に関する情報共有を行う「不正プログラム対策協議会」が設置されている。

の在り方について検討する。

検察や警察分野において、サイバー犯罪に的確に対処するため、人材育成等による取締り等の体制を強化する。

⑥サイバー空間の防衛

国家機密等を窃取・損壊する標的型攻撃や外国政府等による武力攻撃等の一環として行われるサイバー攻撃[96]など外国政府等の関与が疑われる国家レベルのサイバー攻撃が発生した場合について、我が国全体としての対応の強化を図ることが重要である。

具体的には、サイバー攻撃の主体の特定に資する平素からのサイバー攻撃に関するインシデントの認知、インシデント情報等の収集・共有や高度な解析等に関する関係機関の役割の明確化及び体制等の強化とともに、それらの機関間の連携を強化する。

サイバー空間は、自衛隊等による情報収集、攻撃、防御といった様々な活動がその中で行われる、陸・海・空・宇宙と並び得る新たな「領域」であり、その効果的な活動が重要であるとともに、政策策定や部隊運用などの業務で活用され、現実の陸等の領域における様々な活動を支える不可欠のインフラとして、安定的な利用を確保することも重要となっている。

とりわけ、武力攻撃の一環としてサイバー攻撃が行われた場合には、自衛隊等がこれに対処する任務を負っているところであり、この遂行のためには、自らのシステムに対するサイバー攻撃に適切に対処するなどの態勢が必要である。具体的には、DII[97]ネットワークにおける監視態勢、実践的なシミュレーション環境での訓練、サイバー防護分析装置の機能向上等による警戒態勢、サイバー防衛隊（仮称）の新編等による体制、高度の専門性等を有した人材の安定的な確保や高度な研究開発などサイバー空間における自衛隊等の能力・態勢強化に向けた取組等を強化する。

防衛関連システム以外の重要インフラ等の情報システムに対する攻撃における防衛省・自衛隊等の政府機関の役割や海外からの不正通信等に対する

---

96 平成25年3月4日衆議院本会議における内閣総理大臣答弁では、「サイバー攻撃と武力攻撃等との関係については、様々な議論が行われている段階であり、一概に申し上げることは困難」とされている。

97 Defense Information Infrastructure（防衛情報通信基盤）。

サイバー空間関連事業者の役割など、相互支援の在り方を含む非常時における関係機関の役割を整理し、必要な体制・機密情報等の共有システム・制度の整備等を行う。その際、個別具体的な国際法の適用についても併せて整理する。

(2)「活力ある」サイバー空間の構築

サイバー空間の発展性を確保するため、サイバー攻撃への対応の担い手となる産業の活性化、高度な技術の開発、人材やリテラシーの育成・涵養等により、「活力ある」サイバー空間を構築し、サイバー空間を取り巻くリスクに自立的に対応できる創造力・知識力の強化を目指す。

① 産業活性化

新たな成長市場を取り込み、海外市場において収集するサイバー攻撃等に関する動向を踏まえ、新たなリスクに対しより的確かつ迅速に対応していくためには、海外の技術、サービスや製品への依存度が高い我が国のサイバーセキュリティ産業について、国際競争力を強化することが必要である。

高度な技術や製品等と、それらを創り出す先端的な研究者や技術者については、情報通信技術の普及・高度化と、その利活用の進展にとっての不可欠の基盤となるものである。情報通信技術の利活用の裾野拡大による多様な分野におけるサービス革新・生産性の向上や、ビッグデータの活用等による新ビジネスの創出において情報通信技術の利活用が重要となる中、これらと一体となって情報セキュリティ対策に関する高度な技術の研究開発、国際標準化や評価・認証を含んだ制度整備等が必要である。

具体的には、M2M等を基盤としたスマートコミュニティ・スマートグリッド、スマートシティやスマートタウンにおける情報セキュリティ関連技術、パーソナルデータ等を利活用した新サービスを促進するための高セキュアなデバイス技術、匿名化・暗号技術、多種多量のデータについてソフトウェアによりネットワーク全体を制御する技術やサイバー空間上の本人確認技術等に関する研究開発等を強化する。

今後、情報通信技術を利活用した製品やサービスが、国際的な取引において、サイバーセキュリティ上の信頼性を求められるようになる中、それを証明す

るものとして、国際標準化や評価・認証、情報セキュリティ監査の重要性が増してくると考えられる。このため、国際貿易において日本企業が有利になるよう、国際標準化や評価・認証の国際的な相互承認枠組み作り[98]に関して、積極的に参画・働きかけを進めるとともに、国内の評価・認証機能の整備も進めていくことが必要である[99]。具体的には、クラウドコンピューティングサービスにおける国際標準化や、複合機の国際的な共通セキュリティ要件の策定、セキュリティ検証施設[100]を中核とした産業制御システムの評価・認証機関の整備を進めていく。

新たな技術が採用された製品等の調達を政府が積極的に行うことにより、民間企業等における製品開発、実用化や海外市場の獲得等を促進するとともに、ベンチャー企業を育成する。また、情報セキュリティ分野でグローバル競争に対等に伍していくことのできる強い企業を国内に有していく観点から、産業や組織の壁を超えた連携の促進や、潜在力を持つ企業のグローバル展開の支援を図る。

セキュリティ目的のリバースエンジニアリングに関する著作権法の適用明確化や、ビッグデータ解析による高度なサービスの実現等の産業の活性化を阻む可能性がある規制の改革に取り組むことが重要である。

②研究開発

サイバー空間を取り巻くリスクは、サイバー攻撃の複雑・巧妙化に伴い、今後も急激に変化していくものと考えられ、従来の情報セキュリティ対策のままでは、有効な対策の立案・実施に遅れが生じ、効果が急低下する可能性がある。このため、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。

具体的には、我が国自らが最先端の研究開発を保持・向上することを目的に、研究機関等[101]におけるサイバー攻撃の検知機能や高度解析等の向上に

---

98 例えば、脚注 78。
99 サイバーセキュリティの国際標準としては、ISO/IEC 27001 情報セキュリティマネジメントシステム（ISMS）が代表的であり、我が国では、2002 年からの 10 年間で約 4000 組織が認証を取得している。
100 2012 年 3 月 6 日に、技術研究組合 制御システムセキュリティセンター（Control System Security Center: CSSC）が設立されている。
101 例えば、NICT において、解析能力等の向上に向けて、2013 年 4 月、「CYREC（サイレック）」（Cybersecurity Research Center）として、オール・ジャパンの英知を結集したサイバーセキュリティ研究開発拠点を構築し、本格稼働。

向けた技術の研究開発や実証実験を加速させる。

中でも、潜在型のマルウェアなど、情報通信技術の発展に伴い多様化・高度化するサイバー攻撃に対して、有効な革新的技術等が確立できるよう、暗号研究等の情報セキュリティ研究における理論的アプローチの導入を推進するとともに、近未来のサイバー攻撃に対する先端技術の開発に取り組む。また、セキュリティを支える半導体素子等の開発も重要である。

また、国民の情報や権利、社会システム等を保護するため、ICチップの誤作動の抑制等に関する情報セキュリティ対策技術の確立に向けた先端技術の開発に取り組むとともに、SDNの普及により実現するビッグデータを構成する個々のデータやそれを処理するためのソフトウェア等を含んだネットワークシステム全体の信頼性を確保するための技術の研究開発に取り組む。

これらの研究開発等で得られた知見については、産学官で共有を図り、我が国の防御能力の向上を促進する。また、このような取組については、我が国全体の高度情報セキュリティ人材の育成への貢献も期待できるとともに、このような技術は、世界にも展開可能なものになりうることから、我が国発の新産業創出、さらには経済成長にもつながることが期待できる。

③人材育成

我が国のあらゆる活動がサイバー空間に依存している状況においては、政府機関や企業等の対策実施主体が自らの組織を守るために対策を講じる人材を育成するだけでは、深刻化するリスクへの対応が困難となっている。従って、サイバー空間の拡大・浸透に伴う情報通信技術の利活用の広がりにより、高度かつ国際的な人材の裾野を広げていくことが必要である。

現在、国内における情報セキュリティに従事する技術者は、約26.5万人といわれているが、潜在的には約8万人のセキュリティ人材が不足している状態となっている。また、約26.5万人中、必要なスキルを満たしていると考えられる人材は10.5万人強であり、残りの16万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必要があると考えられている[102]。

こうした従来の情報通信技術の利活用におけるセキュリティ人材不足に対応していくことが必要であることに加え、サイバー空間の拡大・浸透に伴う情報通

[102] IPA 試算。

信技術の利活用の広がりにより、新たな課題に対応しなければならない、セキュリティ人材も今後ますます不足してくると考えられ、人材の発掘、育成、活用を進めることが必要となってくる。

こうした人材の量的不足の解消に向け積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題である。こうした人材の確保に関しては、ソフトウェア関連分野における独創的なアイデアや技術、これらを活用する能力を有する優れた個人を発掘育成するための合宿研修や情報セキュリティ人材が実践的技能を競うコンテスト等を官民で連携し、実施する。

我が国におけるサイバーセキュリティ従事者の能力の底上げと、突出した人材の発掘・育成を図っていくためには、社会全体で育成し活用するための仕組みが必要である。具体的には、情報セキュリティ人材と言っても多種多様であり、その求められるスキルは対象となる人材の属性によっても大きく異なることから、スキル標準の改善・活用を通じ、必要とされる能力・知識を明確化していく。

その上で、スキル標準を活用し、実践的な教育プログラム等に関する大学等専門教育課程の充実化、産学連携の強化や、公的資格・能力評価の改善や新設の必要性も含め、セキュリティレベルに対応した多様な資格・能力評価制度の在り方など情報セキュリティ人材として求められるニーズの多様化に応じた検討を行う。

グローバルに活躍できる人材を育成等することが重要であるため、国際会議への参加や海外の専門的な大学院等への留学を支援するとともに、国内における国際会議の招致や開催を推進する。

人材の発掘・育成を、採用・活用につなげていくことも必要である。そのため、政府機関が率先して、情報セキュリティ人材の外部登用を行う。

④リテラシー向上

我が国においては、サイバー空間が、若年層から高齢層といったあらゆる世代や、個人、家庭、職場、公共施設などのあらゆる場面など、実空間における日常生活や社会経済活動等のあらゆる活動に拡大・浸透している。このように全ての一般国民がサイバー空間と共存している状況においては、裾野が広い

一般国民を対象としたリテラシーの向上を継続的に図ることが必要である。また、これは、高度人材育成のための基盤を提供することにも資するものである。

具体的には、初等中等教育段階からの意識啓発を図っていくことが必要であり、標語・ポスターコンクール等参加型の意識啓発事業を実施する。また、初等中等教育段階において、児童生徒の発達段階に応じ、各教科等の指導に当たっては、コンピュータや情報通信ネットワークなどの情報手段を活用できるようにするための学習活動を充実するとともに、情報セキュリティを含む情報モラルに関する教育の積極的な推進等が図られており、今後はさらに、ソフトウェアのプログラミングに関する教育や学習用のデジタル教科書の活用など教育分野における情報通信技術の利活用の促進と一体となった実践的な取組を推進する。

高齢者層における情報セキュリティ対策も今後一層重要となるため、情報セキュリティに関するサポーター等の育成・活用など高齢者に対するきめ細やかなフォローを行うための環境を整備する。

スマートデバイスについては、特に常時、電源が入り、インターネットと接続状態のままで携帯されているスマートフォンにおいて、位置情報等の様々な利用者情報が扱われる一方で、その構造上、情報セキュリティ対策ソフトによる対応の限界等があるため、個々人におけるリテラシーの強化が一層必要となる。

具体的には、スマートフォンへの移行に伴い、その利用率が大幅に拡大しているSNS[103]等、スマートフォンの利用に関する効果的な対策等について、関係事業者等と協力しその確保を図る。さらに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する。

情報通信技術の急速な進化を踏まえれば、一般利用者のリテラシー向上に必要な対策等に関する情報は適時にアップデートしていくことが求められる。このため、政府機関において、サイバー攻撃への対応の取組を通じて集約した情報を蓄積し、これを分析して一般利用者にわかりやすい形にし、広く全国に行き渡る手段で情報提供を行っていくことが重要である。

[103] 情報通信白書によると、スマートフォン移行前後における利用率の変化に関し、SNS については、移行前の 37.9%から移行後には 62.6%へと大幅に拡大している。

(3)「世界を率先する」サイバー空間の構築

グローバルなサイバー空間に対応するため、閣僚レベルによる発信の強化、国際的なルールづくりへの積極的な参画、積極的な海外市場への展開、能力構築支援や信頼醸成措置等により、「世界を率先する」サイバー空間を構築し、グローバルな戦略空間における貢献力・展開力の強化を目指す。

①外交

我が国においては、サイバー空間における情報の自由な流通の確保を基本的な方針とし、これにより、表現の自由等が確保されるとともに、経済成長、等の多様な恩恵を享受してきている。

グローバル化したリスクへの対応は我が国だけでは出来ないため、この方針や、民主主義、基本的人権の尊重及び法の支配といった基本的な価値観を共有する国や地域とのパートナーシップ関係を多角的に構築・強化することが重要である。このため、国際的にも、国家による過度な管理や規制が行われることなく、開放性や相互運用性を確保しつつ、安全で信頼できるサイバー空間を構築するバランスのとれたアプローチを促進するための外交を行っていくことが必要である。

サイバー空間を利用した行為に対する国際法の適用については、サイバー空間における一定の秩序を確保する観点から、従来の国際法がサイバー空間を利用した行為等にも当然適用されることが重要であるため、国連憲章や国際人道法等の個別具体的な国際法の適用について引き続き検討を深める。

サイバー空間においては、外国政府の関与が疑われるサイバー攻撃が海外において実際に発生している一方、攻撃主体の特定が困難であると考えられていることを踏まえ、攻撃主体の誤認など、当事者が意図しない形でのエスカレーションによる不測の事態を回避するため、信頼醸成措置を着実に進める。

これまで二国間協議・対話を行ってきた国及び機関等との協議・対話を継続しつつ、その他の国等との協議・対話又は意見交換も拡大させていく。また、国連における関連会議やARF[104]などの地域的枠組を始めとした多国間協議・

[104] ASEAN Regional Forum。政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラム。

会合等、加えて、政府機関だけでなくマルチステークホルダーが参画するサイバーセキュリティ関連の各種会議やグローバルなコミュニティ等においても「顔の見える」形で積極的に参画する。

サイバー攻撃に対し迅速かつ的確に対処するためには、特に日米安保体制を基軸とした同盟関係にある米国との協力は重要である。今後、サイバー対話等を通じ、最近のサイバー空間をめぐる様々な問題が、安全保障と経済の両方に深くかかわる喫緊の課題であるとの理解の下、脅威認識の共有、共同訓練等の重要インフラ防護を始めとするサイバー領域での具体的対処の在り方、国際的なルールづくりといった分野における議論を深めていく。

②国際展開

グローバルなサイバー空間においては、脆弱な国や地域が踏み台として狙われ、サイバー攻撃が展開されている。サイバー攻撃等のインシデントへの対応など各国等におけるサイバーセキュリティに関する技術的能力等は多様な状況である中、それぞれが一定のインシデント対応能力等を構築していることが、国際社会における共通認識の醸成やサイバー攻撃の抑止につながるものと期待される。

従って、ASEAN地域等における新興国や途上国等と我が国が共に成長できる関係を構築し、これらに対するサイバー攻撃等への対応能力の構築を積極的に支援することが重要である。

具体的には、各国CSIRTの構築支援や、セキュリティマネジメントのノウハウ支援、国際的な意識啓発、諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを構築し、サイバー攻撃の発生を予知し即応を可能とする技術等に関する研究開発プロジェクトを実施し、その対象国を拡大する。

対策の官民連携によるボットウイルス対策など国内における成功事例の紹介や共同プロジェクトの実施、海外の事業者間による机上演習等を図る。

電子政府等における安全性及び信頼性の確保として取り組んでいる暗号評価プロジェクト[105]について、その成果を国内外に発信し、暗号技術の利用促進を図る。

[105] CRYPTREC。

加えて、国際貿易において、あらゆる情報通信技術を利活用した製品・サービスが、サイバーセキュリティ上の安全性を求められるようになる中、産業活性化の観点からは、我が国が強みを持つ複合機や制御システム等の日本製品が不利な扱いを受けることのないよう、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、我が国として積極的に参画、働きかけを進めていく。

また、新興国等に見られる、情報セキュリティの名を借りた輸入制限や国産品優遇措置などの規制に対しては、国際的な貿易ルールに整合するように求めていくと同時に、国内外における関連制度等の整合性の確保を図ることにより、日本企業の国際展開の促進を図る。例えば、パーソナルデータの国際的な流通に関する国内制度の在り方や、新興国等における制度整備支援等による調和のとれた国際ルールの確立への積極的な貢献の在り方等について検討する。

③国際連携

容易に国境を越えて敢行されるサイバー犯罪に効果的に対処するため、国際連携の強化を図る。具体的には、外国捜査機関等とのサイバー犯罪に関する情報交換を継続的に行うとともに、サイバー犯罪に関する最新の捜査手法を修得し、外国捜査機関との連携を強化するため、職員を派遣する。

証拠の収集等のため外国捜査機関からの協力を得る必要がある場合について、外国の捜査機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。

サイバー犯罪対策における国際連携について、我が国はサイバー犯罪条約[106]を締結していることから、この条約の締結国の拡大をはじめとして、迅速かつ効果的な捜査共助等の法執行機関間における連携の強化を図る。

また、国際連携による情報共有を推進し、サイバー攻撃に関するインシデントの国際的な動向を把握することが重要である。具体的には、CSIRT間のサイバー攻撃に関するインシデント情報の共有促進等の運用レベルにおける連

106 「サイバー犯罪に関する条約」。我が国においては、2004年4月に国会で批准の承認、2011年6月の「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（平成23年法律第74号。いわゆるサイバー刑法。）の成立を経て、2012年11月1日に効力が発生。

携[107]の強化を図るとともに、サイバー犯罪に関連する各国の刑事司法制度整備やサイバー犯罪捜査及び訴追に関わる人材育成等を支援する。

相互不信による不測の事態を回避するため、信頼醸成措置を推進することが重要である。このため、我が国の基本的な立場やベストプラクティスを共有する。また、グローバルなインシデントが発生した場合の相互の連絡体制等を平時から構築するとともに、国際共同研究や、複数国間におけるサイバー攻撃対応演習等を実施する。

さらに、接続先となる諸外国等との国際連携にも資するため、我が国と海外とのネットワークの国際接続の冗長化など国際ネットワークの整備を推進する。

4. 推進体制等

(1)推進体制等

NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、GSOCの抜本的な強化を図るとともに、サイバー攻撃に関するインシデントに関する情報等の集約、サイバーセキュリティに関する国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知、政府機関及び独立行政法人等の関連専門機関等に分散している各種機能の有機的な連携による動的な対応等を強化する。その際、国際的なインシデント対応における我が国の窓口となるCSIRT機能の在り方についても併せて検討する。

以上を踏まえ、NISCについては、専門職員の採用や育成等の人事管理による人材の確保や権限等の必要な組織体制を整備することにより、2015年度を目途として「サイバーセキュリティセンター」(仮称)に改組するものとする。

政府機関や重要インフラ事業者等の関係機関間の有機的な連携のための基盤として、サイバー攻撃に関するインシデント情報等の共有を促進することが必要である。このため、攻撃者等に対して秘密とすべき情報について、既存の仕組みも活用しつつ、共有する目的、共有される情報等の内容や共有する

[107] CSIRT の国際間連携については、我が国から NISC、警察庁サイバーフォースセンター、IPA や JPCERT/CC 等が参画している各国の CSIRT 連携のための国際協議会である FIRST (Forum of Incident Response and Security Teams) や、アジア太平洋地域における CSIRT 間連携である APCERT (Asia Pacific Computer Emergency Response Team) 等がある。

者の範囲等に応じた秘密の保持のための枠組みを整備する。

(2)評価等

本戦略に基づく各種取組施策の確実な実施及び各施策間の有機的な連携を確保する観点から、サイバーセキュリティ立国の実現に向けた中長期の目標の管理を行うとともに、本戦略に基づき、2013年度から毎年度の年次計画及び国際分野における総合的な対応を推進するための方針を策定する。

加えて、国内外の環境変化等に的確に対応し、必要に応じて本戦略及びこれに基づく各種施策や、目標管理の持続的な改善を確保するため、本戦略及びそれに基づく年次計画に関する評価等を実施する。その際、各種施策の進捗状況等について、国民の視点による評価が可能な仕組みとする。