サイバーセキュリティ２０１８

2018 年 7 月 25 日

サイバーセキュリティ戦略本部

目　次

はじめに

本書は、我が国のサイバーセキュリティ政策に関する国家戦略であり、今後閣議決定する予定の次期「サイバーセキュリティ戦略」（以下「2018年戦略」という。）に基づく最初の年次計画である。

自由、公正かつ安全なサイバー空間を創出・発展させ、もって「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」に寄与することを目的として、政府が2018年度に実施する具体的な取組を戦略の体系に沿って示すものである。

本書に示す取組を推進するに当たっては、政府機関における連携は元より、重要インフラ事業者や企業、個人といった多様な主体とも連携しつつ、取組を推進していく。

なお、本書は、2018年戦略が閣議決定された時点から効力を生じるものとする。また、本書の記載にかかわらず、我が国を取り巻くサイバーセキュリティに関する情勢に変化が生じた場合には、その内容に応じて、必要な範囲で迅速に相応の取組を策定・実施することとする。

1. 経済社会の活力の向上及び持続的発展

1.1. 新たな価値創出を支えるサイバーセキュリティの推進

(1) 経営層の意識改革

- 経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催による、経営層の意識改革
- 対策の可視化など、経営層に訴求するための施策の推進
- 企業が参照すべき法制度に関する整理

（2018 年戦略より）

(ア)内閣官房において、2016年に決定した「企業経営のためのサイバーセキュリティの考え方」及び2018年に決定した「サイバーセキュリティ人材育成取組方針」を踏まえ、関係府省庁と協力し、サイバーセキュリティ対策の推進に関する以下の取組を行う。

- サイバーセキュリティ対策について経営層が果たすべき役割、持つべき認識についての考え方の共有を図るため、「企業経営のためのサイバーセキュリティの考え方」の見直しを検討する。
- サイバーセキュリティ対策の取組を分かりやすく表現・普及するため、マークやスローガンなどのツールについて検討を行う。
- サイバーセキュリティ対策に関して、経営層が果たすべき役割・認識について、経営層の視点で、経営層自身に分かりやすく説明する人材、いわゆる伝道師の発掘と派遣や産業界と連携した経営層向けのセミナーについて検討を行う。

(イ)経済産業省において、コーポレート・ガバナンス・システムに関する議論の中で、「守り」のリスク管理の一環として、サイバーセキュリティ対策を位置付け、コーポレート・ガバナンス・システムに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付けることを検討する。

(ウ)経済産業省において、取締役会のサイバーセキュリティへの関与を促すとともに、投資家に対するサイバーセキュリティの啓発を行う観点から、上場企業において行われる「取締役会の実効性評価」の評価項目について、サイバーセキュリティへの経営層の関与をその評価項目として組み込むことを促進する。

(エ)経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、設備投資、体制整備、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、「サイバーセキュリティ経営ガイドライン」の普及を図る。

(オ)内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。

(2) サイバーセキュリティに対する投資の推進

- 企業の積極的な情報発信・開示に向けたベストプラクティスの共有やガイドラインの策定
- 情報発信・開示の状況についての継続的な把握・評価
- 投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくり
- 企業に対するサイバーセキュリティの促進策のフォローと措置の検討
- サイバーセキュリティ保険の活用を推進するための方策についての検討

（2018 年戦略より）

(ア)経済産業省において、「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るために、具体的な対策事例や情報共有活動事例等を示すプラクティスを作成する。また、企業がどの程度サイバーセキュリティ対策を実施するかの目安として活用できる可視化ツールを作成する。

(イ)総務省において、ベストプラクティスも盛り込んだ「セキュリティ対策情報開示ガイドライン」（仮称）を策定、公表する。

(ウ)経済産業省において、一定のセキュリティ品質を有するセキュリティサービスを審査登録する体制を整備することにより競争力強化や活用促進を図るなど、サイバーセキュリティの成長産業化に取り組む。

(エ)総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、それに必要となるシステムやサイバーセキュリティ対策製品等の導入に対して税額控除等を措置するコネクテッド・インダストリーズ税制の活用を促すことで、事業者のセキュリティ対策の強化と生産性向上を同時に促進する。

(オ)経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。

(カ)総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

- 先端技術の利用に伴うサイバーセキュリティリスクの分析・明確化とそれに基づくガイドラインの策定や普及等
- 先端技術のリスク分析や脅威への対策に係る研究開発の推進
- セキュリティ・バイ・デザインの考え方を基本とした取組
- 先端技術の利用を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチング、サイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築
- 我が国の高いサイバーセキュリティが確保されたモノやサービス等のトップセールスや展示会等を活用したアピール、国際展開をしやすいビジネス環境の整備

（2018 年戦略より）

(ア)経済産業省において、IPAを通じ、営業秘密保護に関する対策等を推進するため、組織における内部不正防止のためのガイドラインや営業秘密保護ハンドブックの普及推進を図る。

(イ)経済産業省において、企業の情報漏えいの防止に資するため、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」及び「秘密情報の保護ハンドブックのてびき～情報管理も企業力～」についての普及啓発を図る。

(ウ)総務省及び経済産業省において、「クラウドサービス提供における情報セキュリティ対策ガイドライン」、クラウドセキュリティ監査制度等の普及促進を行う。

(エ)経済産業省において、IPAを通じ、サイバーセキュリティビジネスの振興・活性化を図るため、サイバーセキュリティ対策におけるニーズの明確化・具体化、シーズの発掘やビジネスマッチングを行うメンバーを限定しない情報交流の場（コラボレーション・プラットフォーム）を設置する。

(オ)経済産業省において、日本のセキュリティニーズに応じた日本発のサイバーセキュリティ製品・サービスの創出・活用を推進するため、セキュリティ製品・サービスの有効性検証、レーティングを実施できる環境を整備するための検討を行う。

(カ)経済産業省において、IPAを通じ、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況などの実態と動向を把握するための調査・分析を行うとともに、組込みソフトウェアが組み込まれた製品やシステム開発の高信頼化を目的として、システムアプローチによる安全性解析手法の開発・セキュリティ分析手法の検討、コーディング規約策定及びそれらの普及を図る。

(キ)経済産業省において、ASEANをはじめとした新興国に対し、電力をはじめとした重要インフラ分野におけるサイバーセキュリティに関する意識啓発、知見・能力の構築支援を通じて、日本製のセキュリティを備えた質の高いインフラ輸出に向けた環境整備を行う。

1.2. 多様なつながりから価値を生み出すサプライチェーンの実現

(1) サイバーセキュリティ対策指針の策定

- サプライチェーンにおいて、運用レベルでの対策が実施できるような業種横断的な指針の策定
- IoT 機器や組織等に求められる具体的な対応策の産業分野毎の提示

（2018 年戦略より）

(ア)経済産業省において、産業サイバーセキュリティ研究会の下に設置したWG1(制度・技術・標準化)において、Society5.0の実現に必要なセキュリティ対策を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定する。また、産業分野毎に設置したSWGにおける検討を通じて、産業分野毎に守るべきもの・リスク・必要な対策について整理する。

(イ)経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、リスクの高い丸投げ下請や多様化するセキュリティ対策費用の増加に応じた適切な価格設定に向け、セミナー等を通した下請ガイドラインの更なる浸透を図るとともに、業界団体と連携したフォローアップなどを実施し、情報システム開発・運用に係る取引の適

正化を図る。

(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

- 要件の確認等による信頼を創出する仕組みの構築
- 信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築
- トレーサビリティを確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みの検討

（2018 年戦略より）

(ア)内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、中小企業を含むサプライチェーン全体を守ることに活用できる、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進する。本プロジェクトでは、IoT機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。また、本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。

(イ)経済産業省において、業界横断的な指針及び産業ごとの対策を整理した上で、セキュリティ対策が講じられているかどうかを確認するための、認証を含む確認の仕組みを検討する。

(3) 中小企業の取組の促進

- 中小企業を対象としたサイバーセキュリティ対策の事例集の作成
- サイバーセキュリティ保険の活用促進
- 中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化
- 中小企業が自主的に宣言できる仕組みなどの可視化の取組促進、インセンティブの仕組みとの連携

（2018 年戦略より）

(ア)内閣官房において、中小企業における実態を踏まえつつ、ITやセキュリティの知識がなくとも理解できるような対策集の作成に向けた取組を行う。

(イ)総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。（再掲）

(ウ)経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。（再掲）

(エ)経済産業省において、営業秘密保護や事業継続性の観点からも経営層がサイバーリスクを重

要課題として把握し、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、「サイバーセキュリティ経営ガイドライン」の普及を図る。またIPAを通じて、中小企業における情報セキュリティ対策の実施を促すため、説明会等において「中小企業の情報セキュリティ対策ガイドライン」の普及を図る。

(オ)中小企業における情報セキュリティ投資を促進するため、経済産業省において、以下の取組を実施する。

- 中小企業等の生産性向上に資するIT導入の促進とあわせて、セキュリティに係る意識向上やその対策に向けた具体的な取組を促す。
- 認定されたITベンターに対してサイバーセキュリティの情報提供などを実施するとともに、当該ITベンダーが取り組むセキュリティ対策に関する情報を中小企業向けに開示する仕組みの構築を進める。
- 財政投融資制度において、中小企業で導入が進んでいないネットワークセキュリティの更なる普及促進に向けて、特別利率による融資を実施する。

(カ)経済産業省において、IPAを通じ、中小企業における情報セキュリティ教育担当者や中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ講習講師養成セミナー」を実施するとともに、中小企業団体、関係機関等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施する。さらに、IPAが2017年度に創設した、対策ガイドラインに基づき中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」への登録を促すことで、中小企業のセキュリティレベルの向上、IPA等の作成する啓発資料や情報セキュリティ対策支援サイト等のツール等の利用促進等を図る。

1.3. 安全なIoTシステムの構築

(1) IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化

- 各主体の間での共通認識の醸成と、役割や機能の明確化を図った上での、協働した取組の推進
- 官民の各主体が抱える課題やそれぞれの取組の可視化と情報共有を行うための仕組みの構築
- 安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組

（2018 年戦略より）

(ア)内閣官房において、IoTシステムに係る新規事業がセキュリティ・バイ・デザインの考え方に基づき取り組まれるよう、経費の見積もりの方針にこうした考え方を盛り込むとともに、各府省庁等において、こうした考え方に基づく取組が行われるよう働きかけを引き続き行う。さらに着実にこの考え方に基づく取組が行われているか適時確認をする。

(イ)内閣官房において、自律的なIoTシステムに係る関係省庁の取組を推進するとともに、各主体が協働できるよう情報共有等の取組を推進する。その際、各主体の間で共通認識や役割の明確化を図るため、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を踏まえた取組(IoTの分野個別の課題だけでなく、その範囲や定義、物理安全対策、責任分界点（既知の脆弱性への対応に関する製造者責任や運用者等の安全管理義務などインシデント発

生時における関係者の責任を含む）やプライバシーの問題などの共通課題の検討を含む。）を推進する。

(ウ)安全なIoTシステムの構築に向けて、総務省及び経済産業省において、以下の取組を実施する。

- 総務省及び経済産業省において、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC1/SC27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進する。
- 総務省及び経済産業省において、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、「IoTセキュリティガイドライン」を様々な産業分野の標準仕様等に反映させるべく、普及展開に努めるとともに、IoTセキュリティに関する研究開発、実証実験及びIoTセキュリティの確保に向けた総合的な対策の実施を通じ、IoT製品やシステムにおける「セキュリティ・バイ・デザイン」の国際的展開に向けた活動を行う。
- 経済産業省において、IPAを通じて、「IoTセキュリティガイドライン」の考え方の基本となった「つながる世界の開発指針」、又はその他関連ガイド等を様々な産業分野や団体の標準仕様等に反映させるべく、引き続き提案活動を実施する。また「IoTセキュリティガイドライン」を基本とする考え方の国際標準化に向けた取組を進める。
- 経済産業省において、産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下に設置したスマートホームSWG（一般社団法人電子情報技術産業協会スマートホームサイバーセキュリティWG）の場を活用して、家電など家庭で使われるIoT機器のサイバーセキュリティの確保のための必要な対策について、関連する事業者と連携しながら検討を進める。

(エ)内閣官房において、IoTシステムの設計・開発・運用に係る概念について、国内で官民が連携してモノ・ネットワーク、システム等に関する各種基準等への組込みを促進するため、情報技術に関わる国際標準化を担うISO/IECの分科委員会にて2017年11月に日本が提案した「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基本とした国際規格案の標準化に向け、積極的に取り組む。

(2) 脆弱性対策に係る体制の整備

- IoT 機器に必要なサイバーセキュリティに関する要件の整理と、その要件を満たす IoT 機器の利用の推奨
- パスワード設定に不備のある機器の調査・特定を行い、利用者への注意喚起を円滑に行えるような所要の制度整備
- 我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献

（2018 年戦略より）

(ア)内閣官房及び関係省庁において、サイバー環境をよりクリーンなものに保つため、官民が連携して「ボット撲滅」に向けた体制を構築し対策を推進するための検討を行う。

(イ)総務省及び経済産業省において、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、「IoTセキュリティガイドライン」を様々な産業分野の標準仕様等に反映させるべく、普及展開に努める。

(ウ)総務省において、NICTを通じ、パスワード設定に不備のある機器の調査を行い、電気通信事

業者の協力の下、当該機器の利用者を特定し、設定変更を促す取組を行う。また、「IoTセキュリティ総合対策」を踏まえ、2018年度中にIoT機器に対する脆弱性対策に関する実施体制を整備する。

2. 国民が安全で安心して暮らせる社会の実現

2.1. 国民・社会を守るための取組

(1) 安全・安心なサイバー空間の利用環境の構築

・ 脅威に対して事前に積極的な防御策を講じる「積極的サイバー防御」の推進
（2018 年戦略より）

(ア)経済産業省において、経済産業省告示に基づき、IPA（受付機関）とJPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）などを通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、能動的な脆弱性の検出とその調整に関わる取組を行う。また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動をJPCERT/CCにおいて実施する。

(イ)経済産業省において、情報システム等がグローバルに利用される実態に鑑み、IPA等を通じ、脆弱性対策に関するSCAP、CVSS等の国際的な標準化活動等に参画し、情報システム等の国際的な安全性確保に寄与する。

(ウ)経済産業省において、JPCERT/CCを通じて、ソフトウェア等の脆弱性に関する情報を、マネジメントツールが自動的に取り込める形式で配信する等、ユーザー組織における、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び脆弱性マネジメント支援を実施する。

(エ)経済産業省において、IPAを通じ、情報システムの脆弱性に対して、プロアクティブに脆弱性を検出する技術の普及・啓発活動を行う。

(オ)経済産業省において、フィッシング対策協議会及びJPCERT/CCを通じてフィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組等を実施する。

(カ)経済産業省において、IPAを通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。

(キ)経済産業省において、IPAを通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。

(ク)経済産業省において、IPAを通じ、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、「安全なウェブサイトの作り方」を引き続き公開するとともに、体験的かつ実践的に学ぶツール「AppGoat」についてセミナー等を開催することで更なる普及啓発を図る。

(ケ)経済産業省において、JPCERT/CCを通じて、ソフトウェア製品や情報システムの開発段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。

(コ)総務省において、高度化・巧妙化するマルウェアの被害を防止するため、「ICT-ISAC」が中心となって実施している、マルウェアに感染した端末が不正サーバと通信しようとする場合に、当該通信を遮断することで、被害を未然に防止するなどの取組（ACTIVE）を促進する。

(サ)総務省において、2018年５月に成立した電気通信事業者間のサイバー攻撃に関する情報共有の促進のための制度整備を含む「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」を踏まえ、その施行に向けた省令等の整備を行う。

(シ)総務省において、いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC等）の普及を図る。

- サービスの全体の基盤となる信頼できる情報インフラの整備の促進
- 仮想通貨交換業者との連携及び対応の推進
- 自動運転車やドローンに関するセキュリティ対策の推進

（2018 年戦略より）

(ス)内閣官房、総務省及び経済産業省において、情報通信ネットワークの変化、新たなサービス提供に伴い社会・経済に生じ得るリスク源を評価するとともに、情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等について調査を行う。

(セ)重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化すること、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等及び重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。

(ソ)金融庁において、仮想通貨交換業者におけるサイバーセキュリティの強化に向け、認定された自主規制団体との意見交換等を通じて、実効性ある自主規制機能の確立を促していく。

(タ)国土交通省において、独立行政法人自動車技術総合機構交通安全環境研究所と連携し、自動車の安全基準の国際調和等を審議する唯一の場である国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論を議長国として主導するとともに、基準適合性に係る審査体制の構築を図る。

(チ)経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクへの対応に向けて、2018年度中に車両内の電子システムを模擬した評価環境（テストベッド）を構築し、2019年度以降、人材育成等に活用する。

(ツ)内閣府SIP（戦略的イノベーション創造プログラム）を中心に、経済産業省、総務省をはじめとする関係省庁と連携し、2017年度に作成したセキュリティ評価ガイドライン案を踏ま

え、実証実験を実施する。

(テ)様々な用途への活用が進むドローンのサイバーセキュリティについて、内閣官房及び関係省庁等による「小型無人機に係る環境整備に向けた官民協議会」等の場において、「空の産業革命に向けたロードマップ2018～小型無人機の安全な利活用のための技術開発と環境整備～」(2018年６月小型無人機に係る環境整備に向けた官民協議会決定）に基づき、空の産業革命に向けた総合的な検討の一環として論点整理を行う。

(2) サイバー犯罪への対策

- サイバー犯罪の実態把握、取締りの推進
- 官民が連携したサイバー犯罪対策の推進
- サイバー空間における事後追跡可能性の確保に必要な取組の実施

（2018 年戦略より）

(ア)警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等を対象として、情報セキュリティに関する意識・知識の向上、サイバー犯罪による被害の防止等を図るため、サイバー犯罪の現状や検挙事例、スマートフォン等の情報端末やSNS等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。さらに、関係省庁との連携によるスマートフォンに関する青少年に対する有害環境対策の徹底等、スマートフォンの安全利用のための環境整備に向けた取組を実施する。

(イ)警察庁、総務省及び経済産業省において、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為、フィッシング行為、他人の識別符号を不正に取得・保管する行為等の取締りを強化するとともに、事業者団体に対する不正アクセス行為の手口に関する最新情報の提供や、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況の公表等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図るなど、官民連携した不正アクセス防止対策を更に推進する。

(ウ)警察庁において、サイバー防犯ボランティアの結成を促すとともに活動の支援を強化することにより、安全で安心なインターネット空間の醸成に向けた取組を推進する。

(エ)警察庁において、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、サイバー犯罪等の取締りのための情報技術の解析に関する研究及びサイバー犯罪等の取締りに必要な専門的知識・技術に関する研修を実施する。

(オ)警察庁において、高度な情報通信技術を用いた犯罪に対処するため、情報技術の解析に関する資機材の強化、関係会合への参加、技術協力を通じた関係機関との協力、不正プログラムの解析等を推進する。また、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、新たな電子機器や技術に係る解析手法の確立に向けた研究を推進する。

(カ)法務省において、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。

(キ)検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに、サイバー犯

罪に関する条約を締結するための「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」（サイバー刑法）の適正な運用を実施する。

(ク)総務省において、NICTを通じ、能動的・網羅的なサイバー攻撃観測技術の開発に取り組むとともに、運用するサイバー攻撃観測網（NICTER）における観測・分析結果をNISCをはじめとする政府機関等への情報提供等を通じた連携強化を図る。

(ケ)経済産業省において、産業界及び関係省庁と連携し、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、「営業秘密官民フォーラム」を開催するとともに、参加団体等に営業秘密に関するメールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行う。

(コ)警察庁において、新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）の悪用等急速に悪質巧妙化するサイバー犯罪の取締りを推進するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内研修及び民間企業への講義委託の積極的な実施、官民人事交流の推進、技術的に高度な民間資格の活用等、サイバー犯罪への対処態勢を強化する。

(サ)警察庁において、サイバー空間の脅威に対処するため、日本版NCFTAである一般財団法人日本サイバー犯罪対策センター（JC3）や、都道府県警察と関係事業者から成る各種協議会等を通じた産学官連携を促進するとともに、サイバーセキュリティ政策会議等において官民連携による取組を推進する。

(シ)経済産業省において、フィッシング詐欺被害の抑制のため、フィッシング対策協議会を通じて、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を行う。

(ス)警察庁において、公衆無線LANを悪用したサイバー犯罪に対する事後追跡可能性の確保に必要な対策が適切に講じられるよう、必要な対応を行う。

(セ)警察庁及び総務省において、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」の解説を踏まえ、関係事業者における適切な取組を推進するなど必要な対応を行う。

2.2. 官民一体となった重要インフラの防護

(1) 行動計画に基づく主な取組

- 重要インフラ行動計画に基づく取組の推進及び同計画の見直し
- 面としての防護の強化及び情報共有の促進・拡充

（2018 年戦略より）

(ア)内閣官房及び重要インフラ所管省庁等において、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の５つの施策を実施する。

- 「安全基準等の整備及び浸透」については、重要インフラ各分野に横断的な指針の策定とそれに基づく、各分野の「安全基準」等の整備・浸透を促進する。
- 「情報共有体制の強化」については、連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化を行う。
- 「障害対応体制の強化」については、官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化を行う。
- 「リスクマネジメント及び対処態勢の整備」については、リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援を行う。
- 「防護基盤の強化」については、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等を推進する。

(イ)総務省において、重要インフラにおけるサービスの持続的な提供に向け、重要無線通信妨害事案の発生時の対応強化のため、申告受付の24時間体制を継続して実施するとともに、妨害原因の排除を迅速に実施する。また、重要無線通信への妨害を未然に防ぐための周知啓発を実施するほか、必要な電波監視施設の整備、電波監視技術に関する調査・検討を実施する。

(ウ)経済産業省において、安全・安心なクレジットカードの利用環境の整備を目的とする「割賦販売法の一部を改正する法律（平成28年法律第99号)」の成立を受け、2017年12月に改正政省令を公布し、2018年６月に改正法を施行する。また、クレジットカード取引に関係する事業者等で構成されているクレジット取引セキュリティ対策協議会において、改正法の実務上の指針として、2018年３月に改訂された「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2018-」に基づき、関係事業者等の取組を更に推進する。

(エ)厚生労働省において、「未来投資戦略」等に基づき、保健医療記録共有サービスを2020年度から本格稼働させることを目指す中で、ネットワークや医療機関のセキュリティ対策強化について、コスト負担のあり方も含めて調査・検討する。

(オ)厚生労働省において、医師等の医療従事者が資格を証明できる電子証明書である保健医療福祉分野電子証明書（HPKI）の活用・普及について一層推進していく。

(カ)厚生労働省において、医療機器の安全性を担う医療機器製造販売業者、組織としての対策を行う医療機関、脆弱性や攻撃の分析を行うセキュリティ機関、自治体等と連携・協調して対応する。

(キ)スマートメーターシステムセキュリティガイドラインに基づき電力各社が取組を強化している中で、経済産業省において、スマートメーターのセキュリティを含め電力会社を取り巻く情勢を分析し、課題の抽出及び必要な対策を検討すべく、新たに有識者が参画する専門の研究会（電力サブワーキング）を立ち上げる。

(ク)内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に基づく施策を、中小事業者へ拡大すると共に、継続的に重要インフラに係る防護範囲の見直しに取り組む。

(ケ)総務省において、NICTを通じ、標的型攻撃に関する情報の収集・分析能力の向上に向け、官公庁・大企業のLAN環境を模擬した実証環境を用いて標的型攻撃の解析を実施する。また、「ICT-ISAC」が中心となって実施している、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの構築及び関係事業者等での情報共有の取組を促進する。

(コ)内閣官房において、情報セキュリティ関係機関等と協力関係を構築・強化していくと共に、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、情報セキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を行う。

① リスクマネジメントの推進
・ リスクマネジメントの活動全体が継続的かつ有効に機能することに資する取組の推進
（2018 年戦略より）

(サ)内閣官房において、重要インフラサービスを安全かつ持続的に提供できるよう、重要インフラサービス障害の発生を可能な限り減らすとともに、迅速な復旧が可能となるよう、情報セキュリティ対策に関する取組を推進する。また、オリパラ大会に関係する重要なサービスについても、安全かつ持続的に提供できるよう、この取組を推進する。
- 重要インフラ事業者等における平時のリスクアセスメントに対し、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」に基づくリスクアセスメントの実施（継続的な見直しを含む）の浸透に向けた取組を行う。
- 重要インフラ事業者等の事業継続計画及びコンティンジェンシープランに対し、盛り込まれるべき「サイバー攻撃リスクの特性並びに対応及び対策の考慮事項」の浸透に向けた取組を行う。

(シ)金融庁において、大規模な金融機関に対して、そのサイバーセキュリティ対応能力をもう一段引き上げるため、「脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）」等、より高度な評価手法の活用を促していく。

② 安全基準等の改善・浸透
・ 安全基準等を改善する取組の継続的な推進
・ 安全等を維持する観点を踏まえた制度的枠組みの適切な改善
（2018 年戦略より）

(ス)重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化すること、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等及び重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。(再掲)

(セ)総務省において、ネットワークIP化の進展に対応して、ICTサービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。

(ソ)総務省及び経済産業省において、重要インフラ事業者等が保有する重要データがクラウドサービス等において適切に保護される仕組みの在り方について本年度中に国内外の実態調査を踏まえ技術面・法制度面から検討を開始する。

(タ)厚生労働省において、医療機関におけるサイバーセキュリティの現状について調査を行うとともに、医療情報システムの安全管理ガイドラインの普及に取り組む。

(チ)厚生労働省において、医療機器のサイバーセキュリティ対策ガイドラインの策定等により、医療機器のサイバーセキュリティ対策を推進していく。

(ツ)経済産業省において、「ガス事業法」により、ガス事業者に作成と遵守が課せられる保安規程の規定事項に「製造・供給に係る制御システムのサイバーセキュリティ対策」を追加することについて具体化を図る。

③ 深刻度評価基準
・ サイバー攻撃による重要インフラサービス障害等に係る深刻度評価基準の策定
(2018 年戦略より)

(テ)内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に従い、情報共有体制の強化について次のとおり検討を進める。
- サービス障害の深刻度評価基準の導入に向けた検討を進める。
- 連絡形態の多様化（連絡元の匿名化、セプター事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除、及び分野横断的な情報を内閣官房に集約する仕組みの検討を進める。
- 効果的かつ迅速な情報共有に資するため、情報共有システム構築に係る検討を行う。

④ 官民の枠を超えた訓練・演習の実施
・ 官民の枠を超えた様々な規模の主体間での訓練・演習の実施
(2018 年戦略より)

(ト)情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。
- 内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施する。
- 総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。
- 金融庁において、参加金融機関および金融業界全体のセキュリティレベルの底上げを図るため、攻撃の実例分析を踏まえた金融業界横断的なサイバーセキュリティ演習について、必要に応じて対象業態を拡充の上、引き続き実施する。

⑤　制御系システムのセキュリティ対策
・　制御系システムの特性を踏まえたセキュリティ対策の実施
・　制御系システムに関する人材育成及び脅威情報の収集・分析・展開等の推進
（2018 年戦略より）

(ナ)経済産業省において、JPCERT/CCを通じて、インターネット上の公開情報を分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの脆弱性や設定の状況について、その保有組織に対して情報を提供する。

(ニ)経済産業省において、制御システムのテスト環境を用いシステム全体の脅威分析、リスク評価を行う技術開発を行う。

(ヌ)内閣官房において、我が国で使用される制御系機器・システムに関する脆弱性情報やサイバー攻撃情報などの有益な情報について、非制御系の情報共有体制と整合性のとれた情報共有体制により、収集・分析・展開していく。また、どのような情報が事業者等にとって有益なのかヒアリング等により調査し、情報共有がより効果的なものとなるよう検討を行う。

(ネ)経済産業省において、海外におけるルール化の動向も踏まえ、サプライチェーンにおける脅威を明確化し、運用レベルでの対策が実施できるような業種横断的な指針を策定するとともに、重要産業分野を中心に産業分野毎のサプライチェーンの構造や守るべきもの、脅威の差異を考慮した、産業分野別の具体的な対策指針を策定する。

(2) 地方公共団体のセキュリティ強化・充実

・　サービス障害や人為的ミスによるマイナンバーを含む情報漏えいへの対策
・　セキュリティポリシーに関するガイドラインの更新
・　業務用ネットワークのセキュリティレベルの確保
・　セキュリティ人材の確保・育成及び体制の充実を支援する取組の推進
・　官民の認証連携に関する環境整備
（2018 年戦略より）

(ア)内閣官房及び総務省において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対する情報の提供など、地方公共団体におけるサイバーセキュリティの確保のために必要とされる協力を行う。

(イ)総務省において、関係機関と協力の上、地方公共団体職員が情報セキュリティ対策について習得することを支援するため、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーを集合研修で、その他情報セキュリティ関連研修をeラーニングで実施する。また、マイナンバー制度における情報連携の状況等を踏まえつつ、地方公共団体における情報セキュリティポリシーに関するガイドラインの改定を実施する。

(ウ)総務省において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。

(エ)総務省において、関係機関と協力の上、サーバやネットワーク機器等における脆弱性診断を地方公共団体自らが実施できるよう支援する。地方公共団体の対策やリソースの充実を図るべく、緊急時対応訓練の支援及びCSIRTの連携組織を設立し、地方公共団体のインシデント即応体制の強化を図る。

(オ)内閣官房及び総務省において、総合行政ネットワーク（LGWAN）に設けた集中的にセキュリティ監視を行う機能（LGWAN-SOC)などにより、GSOCとの情報連携を通じた、国・地方全体を俯瞰した監視・検知を行う。また、総務省において、地方公共団体のセキュリティ強化対策を推進するため、情報システムの強靭性の向上や自治体情報セキュリティクラウドの状況に係るフォローアップを実施するとともに、「自治体情報セキュリティ向上プラットフォーム」の利用を促進することにより、マイナンバー制度を含めたセキュリティ確保を徹底する。さらに、情報連携に利用する情報提供ネットワークシステムについて、インターネットから独立する等の対策を講じており、引き続き高いセキュリティ確保をすべく、適切な管理・監督・支援等を行う。加えて、個人情報保護委員会において、関係省庁等と連携しつつ、特定個人情報の適正な取扱いに関するガイドラインの遵守、特定個人情報に係るセキュリティの確保を図るため、専門的・技術的知見を有する体制を拡充するとともに、監視・監督機能を強化し、情報提供ネットワークシステムに係る監視を適切に行う。

(カ)総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、地方公共団体におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。

(キ)内閣府において、2017年11月に本格運用を開始したマイナポータルを活用し、官民の認証連携をより一層推進していく。

(ク)厚生労働省において、マイナンバーカードの健康保険証としての活用について、2020年度の導入を目指して準備を進めていく。

2.3. 政府機関等におけるセキュリティ強化・充実

(1) 情報システムのセキュリティ対策の高度化・可視化

- 対処能力の向上に加え、新たな防御技術を活用したより効果的な取組
- 情報システムの防御能力の向上と状態の把握
- 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

（2018 年戦略より）

(ア)内閣官房において、統一基準群の改定に伴う各府省庁、独立行政法人及びサイバーセキュリティ基本法に基づく指定法人（以下「独立行政法人等」という。）の情報セキュリティポリシーの見直しについて、必要な支援を行う。また、新たに直面した脅威・課題への対応について、統一基準群の将来の改定に向けた知見の蓄積を行う。

(イ)内閣官房において、政府機関等の情報システムの調達におけるセキュリティ・バイ・デザインを推進するため、NISCが公表しているセキュリティ・バイ・デザインに関連するマニュアルの改定に着手する。

(ウ)経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPAを通じ、

「IT製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。

(エ)経済産業省において、IPAを通じ、CCRAなどの海外連携、セキュリティ評価に係る国際基準の作成や各国の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。

(オ)経済産業省において、IPAを通じ、JISEC（ITセキュリティ評価及び認証制度）の利用者の視点に立った評価・認証手続の改善、積極的な広報活動等を実施するとともに、安全な政府調達を推進するため、調達関係者に対する広報活動や勉強会、ヒアリングを実施するとともに必要に応じて手順や新たなIT製品への対応等の見直しを実施する。

(カ)経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するためIPAの運用する暗号モジュール試験及び認証制度（JCMVP）の普及を図る。

(キ)内閣官房において、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府機関情報システムのサイバー攻撃等に関する情報を24時間365日収集・分析し、政府機関等に対する新たなサイバー攻撃の傾向や情勢等について、分析結果を各政府機関等に対して適宜提供する。また、IPAの実施する、独立行政法人等に係る監視業務の監督を行うとともに、監視に係る能力や機能の向上の観点から、攻撃情報の共有等の連携を図る。

(ク)内閣官房において、巧妙化する情報セキュリティに関する脅威、動向等を踏まえ、各府省庁の情報システムにおける対策の実施状況の点検・改善を行うため、公開された脆弱性等への対応やサイバー攻撃に係る対策の実施状況の調査を行う。調査結果は、マネジメント監査により確認された課題等も踏まえ、統一基準群を始めとした規程への反映や改善に向けた取組について検討を行う。

(ケ)内閣官房において、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用等を通じて標的型攻撃に対する多重防御の取組を引き続き推進する。

(コ)内閣官房において、大規模サイバー攻撃や大規模災害発生時における、情報システムを用いる業務についての復旧対策を強化するため、政府機関におけるIT-BCPの見直しにかかる調査等を実施するとともに、規程の改定に着手する。

(サ)総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、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、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。

(シ)厚生労働省において、社会保険診療報酬支払基金のサイバーセキュリティ体制について、内閣官房等と緊密に連携し、迅速なサイバー攻撃からの防護の技術的な体制の強化に取り組む。

(ス)内閣官房において、2020年東京オリンピック・パラリンピック競技大会及びその後を見据え

て、インシデント発生前及び発生時の情報提供の迅速化・高度化に資するGSOCシステムの検知・解析機能を始めとした機能強化、GSOCセンサーの増強等の検討を行うなど、政府機関等における端末等での新たな監視手法等の導入状況を踏まえつつ、政府機関等と次期GSOCにおける効果的かつ効率的な連携を推進する。

(2) クラウド化の推進等による効果的なセキュリティ対策

- 政府プライベート・クラウドとしての政府共通プラットフォームへの移行を含むクラウド化の推進
- 信頼できるクラウドの利用を促進する方策の検討
- 政府機関のインターネット接続口の適切な集約の推進とともに、境界監視ポイントの集約の検討

（2018 年戦略より）

(ア)政府機関のクラウド化を推進する観点から、以下の取組を行う。
- 内閣官房において、政府機関におけるクラウドサービスの利用状況を適宜調査し、課題等の把握に努める。
- 総務省において、政府共通プラットフォームの本格更改に向け、新たな政府のプライベート・クラウドとしての整備計画を策定する。

(イ)総務省及び経済産業省において、官民双方が一層安心・安全にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、2018年度から検討を開始する。

(ウ)内閣官房及び総務省において、政府機関のインターネット接続口の集約を推進し、GSOCによる境界監視の効率化を検討する。

(3) 先端技術の活用による先取り対応への挑戦

- 新しい設計思想の下で誕生した情報技術の活用の可能性の検討

（2018 年戦略より）

(ア)内閣官房において、近年普及してきた情報システムの基盤の中でサイバー攻撃による高い耐性を有するものについて、これらの情報技術を、政府機関等において活用できる可能性について検証する。

(4) 監査を通じたサイバーセキュリティの水準の向上

- 組織横断的な分析により抽出される傾向や課題を踏まえたサイバーセキュリティ水準向上の促進
- IT 資産管理情報を活用した効果的かつ効率的な監査の実施

（2018 年戦略より）

(ア)内閣官房において、政府機関における統一基準群等に基づく施策の取組状況について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、自律的なセキュリティ水準の向上を促す仕組みを確立するため、引き続き国の行政機関に対して監査を実施する。監査の実施に当たっては、２年間で全ての国の行政機関に対して監査を実施する計画とし、国の行政機関のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監査を実施した国の行政機関については、フォローアップを実施する。2018年度の監査については、前回までの監査の結果を踏まえるとともに前回対象としなかった部局やシステムを対象として実施する。

(イ)内閣官房において、国の行政機関の情報システムにおけるセキュリティ対策の点検・改善を行うため、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを引き続き国の行政機関に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。なお、ペネトレーションテストを実施した国の行政機関については、フォローアップを実施する。加えて、情報システムのペネトレーションテストを行うに当たり、自衛隊が有する知識・経験の活用を実施していく。

(ウ)内閣官房において、独立行政法人等における統一基準群に基づく施策の取組について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、自律的なセキュリティ水準の向上を促す仕組みを確立するため、IPAとの連携等により、引き続き独立行政法人等に対して監査を実施する。監査は、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う計画とし、独立行政法人等のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監査を実施した法人については、フォローアップを実施する。また、独立行政法人等における情報セキュリティ対策の実施状況を明らかにし、その結果を踏まえ、所管する府省庁と協力しセキュリティ対策の強化を図る。2018年度の監査については、独立行政法人等の業務内容の多様性を踏まえ選定した部署やシステムを対象として実施する。

(エ)内閣官房において、独立行政法人等の情報システムにおけるセキュリティ対策の点検・改善を行うため、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを、IPAとの連携等により、引き続き独立行政法人等に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。ペネトレーションテストは、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う。なお、ペネトレーションテストを実施した法人については、フォローアップを実施する。

(5) 組織的な対応能力の充実

- 事案対応を行うチームを中心に事案対応能力や情報セキュリティに係る知識の向上
- 情報セキュリティ緊急支援チームの要員の対処能力の向上

（2018 年戦略より）

(ア)内閣官房において、サイバーセキュリティ基本法に基づく重大インシデント等に係る原因究明調査をより適切に実施するため、デジタルフォレンジック調査に当たる職員の技術力の向上に引き続き取り組むとともに、民間事業者の知見を活用するための方策を講じる。

(イ)内閣官房において、サイバー攻撃への対処に関する政府機関全体としての体制を強化するため、各府省庁のインシデント対処に関わる要員による情報共有及び連携の促進に資するコミュニティの更なる活性化を図る。

(ウ)内閣官房において、引き続き、府省庁及び独立行政法人等を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の合同研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。

(エ)政府機関におけるサイバー攻撃に係る対処要員の能力及び連携の強化を図るため、以下の訓練・演習を実施する。

- 内閣官房において、各府省庁における情報セキュリティインシデント対処に関わる要員を対象として、最高情報セキュリティ責任者及びサイバーセキュリティ・情報化審議官等をはじめとした幹部による指揮の下での組織的かつ適切な対処の実現を目指し、これまでの訓練や調査等により明らかになった課題や近年のサイバー攻撃動向等を踏まえた訓練を実施する。また、府省庁及び独立行政法人等における情報セキュリティインシデント対処に関わる要員を対象として、研修を年間を通じて実施する。さらに、政府機関等において自組織の環境に最適化した訓練を独自に実施できるようにするために必要な支援を行う。
- 内閣官房において、サイバー攻撃等により発生した支援対象機関等の情報システム障害又はその発生が予想される場合等、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、情報セキュリティ緊急支援チーム（CYMAT）要員等に対する研修と実習等を実施する。
- 総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、国の行政機関等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。
- 内閣官房及び総務省において、昨今のサイバー攻撃やこれまでの実施結果を踏まえつつ、NATIONAL 318(CYBER) EKIDENを実施する。

2.4. 大学等における安全・安心な教育・研究環境の確保

(1) 大学等の多様性を踏まえた対策の推進

- 大学等における計画等に基づく自律的かつ組織的な取組の促進
- サイバーセキュリティに関するガイドライン等の策定と普及
- 各層別研修及び実践的な訓練や演習の実施
- 事案発生時の初動対応への支援

（2018 年戦略より）

(ア)文部科学省において、大学等の多様性を踏まえ、大学等が自律的かつ組織的に取り組むべきサイバーセキュリティ対策について検討を行い、大学等の取組を促進する。また、当該対策の推進に資するガイドライン等について検討する。

(イ)文部科学省において、大学等におけるリスクマネジメントや事案対応に資する各層別研修及び実践的な訓練・演習の体系について検討し、試行的に実施する。

(ウ)文部科学省において、外部のセキュリティ機関等と連携し、大学等で発生した事案の初動対

応について必要に応じて支援する体制を整備する。

(2) 大学等の連携協力による取組の推進

- サイバー攻撃への監視能力の機能維持・強化
- 戦略マネジメント層の育成に向けた共同研究や技術職員への研修の実施
- サイバー攻撃に関する情報や共通課題事案対応の知見等を共有するための取組への支援

（2018 年戦略より）

(ア)文部科学省において、国立情報学研究所（NII）を通じ、国立大学法人及び大学共同利用機関法人（以下「国立大学法人等」という）のインシデント対応体制を高度化するために、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施する。

(イ)文部科学省において、国立情報学研究所（NII）を通じ、サイバー攻撃耐性を向上させるため、国立大学法人等において、M2Mを含み学術評価に適したデータを実環境から継続的に収集し、データ解析技術の開発を促進する。

(ウ)文部科学省において、サイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための手法を検討する。

2.5. 2020年東京大会とその後を見据えた取組

(1) 2020年東京大会に向けた態勢の整備

- 「セキュリティ幹事会」で決定された基本戦略に基づく取組の推進
- 大会の安全に関する情報の集約等の取組の推進
- リスク評価及び明らかになったリスクへの対策の促進
- 「サイバーセキュリティ対処調整センター」の構築の推進と連絡調整態勢の整備

（2018 年戦略より）

(ア)内閣官房において、「2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」（2017年３月21日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。具体的には、オリパラ競技大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象として、リスク評価に基づく対策の促進と、情報の共有、インシデント発生時の調整役となるための組織であるサイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の整備を推進する。2018年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。また、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）については、2018年度末を目途に構築し、2019年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。

(イ)警察庁に設置したセキュリティ情報センターにおいて、国の関係機関の協力を得て、サイバーセキュリティに係るものを含む2020年東京オリンピック・パラリンピック競技大会の安全に関する情報を集約するとともに、大会の安全に対する脅威及びリスクの分析、評価を行

い、国の関係機関等に対し必要な情報を随時提供する。

(2) 未来につながる成果の継承

- 2020 年東京大会の態勢整備のための各種施策の継続推進
- 整備した仕組み、運用経験及びノウハウの活用
- 「サイバーセキュリティ対処調整センター」のナショナル CSIRT としての活用
- 「リスクアセスメント」の手法の全国の事業者等への適用とそのための整備・普及

（2018 年戦略より）

(ア)内閣官房において、2020年東京大会に向けた態勢の整備に当たっては、整備した仕組み、その運用経験及びノウハウが、レガシーとして、2020年東京大会以降の我が国の持続的なサイバーセキュリティの強化のために活用できることを考慮し、構築した「サイバーセキュリティ対処調整センター」は、サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口となる組織（ナショナルCSIRT）へと成長・発展させ、サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう検討する。

(イ)警察庁及び都道府県警察において、2020年東京大会その他の大規模国際イベントを見据えたサイバー攻撃対策を推進するとともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を図る。また、法務省において、人的情報収集・分析を行い、対応を推進する。

(ウ)総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、2020年東京オリンピック・パラリンピック競技大会に向けた大規模演習環境「サイバーコロッセオ」を活用し、同大会のサイバーセキュリティを守る高度な人材の育成を推進し、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図る。

2.6. 従来の枠を超えた情報共有・連携体制の構築

- ISAC を含む既存の情報共有の推進

（2018 年戦略より）

(ア)内閣官房において、情報セキュリティ関係機関等と協力関係を構築・強化していくと共に、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、情報セキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を行う。

(イ)経済産業省において、最新の脅威情報やインシデント情報等の共有のためIPAを通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう参加組織の拡大、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。また、重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、IPAを通じ、障害事例等の情報を重要インフラ事業者等へ提供する。

(ウ)総務省において、ISP事業者やICTベンダー等を中心に構成されている「ICT-ISAC」を核として、国際連携を含めてサイバー攻撃に関する情報共有網の拡充を推進する。

(エ)国土交通省において、2018年４月から重要インフラ（航空、鉄道、物流分野）事業者による情報共有・分析及び対策を連携して行う体制である「交通ISAC」（仮称）の仮運用が開始されたことから、事業者等が参加する検討会を開催し、交通ISACの本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論する。

(オ)金融庁において、金融機関に対し、「金融ISAC」を含む情報共有機関等を通じた情報共有網の拡充を進める。

(カ)厚生労働省において、医療分野及び水道分野のISACについて、必要な調査・情報収集を行うとともに、検討を進める。

(キ)経済産業省において、クレジットカード会社に対し、「金融ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。

(ク)経済産業省において、自動車業界の事業者に対し、「J-Auto-ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。

(ケ)経済産業省において、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供する。

(コ)警察庁において、サイバー空間の脅威に対処するため、一般財団法人日本サイバー犯罪対策センター（JC3）を通じた産学官連携した取組を進める。

(1) 多様な主体の情報共有・連携の推進

- 情報共有に十分な知見を有する専門機関を含む官民の多様な参加主体が、安心して相互に情報共有を図るための体制の構築
- 官民、業界、国内外といった枠を超えた情報共有・連携の推進
- 既存の情報共有体制についての連携や統合の検討

（2018 年戦略より）

(ア)国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための協議会の創設に向けて検討を進める。

(2) 情報共有・連携の新たな段階へ

- 積極的に情報提供に協力する者ほど恩恵を享受できる仕組みの検討
- 情報処理の自動化の推進
- 参加主体が従来の枠を超えて共存・発展する関係構築に向けた環境整備の推進

（2018 年戦略より）

(ア)内閣官房が中心となり構築する情報共有体制において、積極的にサイバーセキュリティインシデント等に係る情報（例えば、リコールの要因となる情報など、国民の生命・身体を保護するために提供される情報を含む。）の共有に貢献する参加者が評価される環境を整備する

ための検討を進める。また、当該体制において情報の共有や分析を迅速に行うための処理の自動化に向けた検討を進める。

(イ)内閣官房が中心となり構築する情報共有体制において、所管省庁を同じくする複数の業界が業界を跨いで情報共有の仕組みを構築する等新しい情報共有・連携を推進するための検討を進める。

2.7. 大規模サイバー攻撃事態等への対処態勢の強化

- サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化
- サイバー空間における情報収集・分析機能及び緊急対処能力の向上

（2018 年戦略より）

(ア)内閣官房において、国民の生命等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（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、関係府省庁、重要インフラ事業者等と連携した初動対処訓練を実施する。

(イ)内閣官房において、サイバー攻撃等の事象に関する政府としての一連の初動対処（検知、判断、対処、報告）を見直し、サイバーセキュリティに係る危機管理対応の一層の強化が図られるよう留意する。

(ウ)警察庁及び都道府県警察において以下の取組を推進することにより、サイバー攻撃対処態勢の強化を図る。

- 都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を図る。
- 警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。
- 警察庁及び都道府県警察において、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を図る。
- 警察庁において、都道府県警察のサイバー攻撃対策担当者を対象に、大規模産業型制御システムに関するサイバー攻撃対策に係る訓練を実施する。
- 警察庁において、サイバー空間の脅威への危機管理に臨むため、サイバー空間に関する観測機能の強化等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。また、サイバー攻撃の実態解明に必要不可欠な不正プログラム等の解析を推進する。

(エ)経済産業省において、JPCERT/CCを通じ、重要インフラ事業者等からの依頼に応じ、国際的なCSIRT間連携の枠組みも利用しながら、攻撃元の国に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。

(オ)経済産業省において、IPAを通じ、我が国経済社会に被害をもたらすおそれが強く、一組織で対処が困難なサイバー攻撃を受けた組織等を支援するため、「サイバーレスキュー隊（J-CRAT)」の活動を増強し、被害組織における迅速な対応・復旧に向けた計画作りを支援す

る。

(カ)個人情報保護委員会において、個人情報取扱事業者における、外部からの不正アクセス等による個人データの漏えい等の事案への対応が適切に実施されるよう、個人情報サイバーセキュリティ連携会議を通じて、関係機関と緊密な連携を図り事案の詳細の把握に努めるとともに、必要に応じて指導・助言等を行う。

(キ)経済産業省において、JPCERT/CCを通じ、企業へのサイバー攻撃等への対応能力向上に向けて、国内における組織内CSIRT設立を促進・支援する。また、CSIRTの構築・運用に関するマテリアルや、インシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRTの普及や、国内外の組織内CSIRTとの間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭においた運用の普及、連携を進める。

3. 国際社会の平和・安定及び我が国の安全保障への寄与

3.1. 自由、公正かつ安全なサイバー空間の堅持

・ グローバル規模で自由、公正かつ安全なサイバー空間を実現するための、国際場裡における理念の発信、サイバー空間における法の支配の推進

（2018 年戦略より）

(ア)内閣官房、外務省及び関係府省庁において、ハイレベルの会談・協議等を通じ、サイバー空間における我が国の利益が達成されるよう、戦略的な取組を進める。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

・ 日本型のサイバーセキュリティの基本的な在り方の発信、サイバー空間の発展を妨げるような国際ルールの変更等を目指す取組への対抗

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、各二国間協議や多国間協議に参画し、我が国の意見表明や情報発信に努めるとともに、越境データ規制、ソースコード開示、国家によるインターネットの資源管理等、自由な情報の流通を阻害するような動きに対抗し、自由、公正かつ安全なサイバー空間を実現する。

(イ)経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（「Forced Localization Measures」）を行う諸外国に対し、対話や意見交換を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、民間団体とも連携しつつ働きかけを行う。

(2) サイバー空間における法の支配の推進

・ 既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論への積極的な関与

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、各二国間協議や多国間協議に参画し、サイバー空間における国際法の適用や国際的なルール・規範作り等に積極的に関与し、それらに我が国の意向を反映させる。

・ サイバー犯罪に関する条約、刑事共助条約、ICPO 等の枠組みを活用した国際機関、外国法執行機関、外国治安情報機関等との間における国際捜査共助や情報交換等による国際連携

（2018 年戦略より）

(イ)警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU、日・露間の刑事共助条約・協定及びサイバー犯罪に関する条約の発効を受け、これらの条約・協定の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。今後は、更なる刑事共助条約の締結について検討していく。

(ウ)警察庁において、迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化を目的とし、我が国のサイバー犯罪情勢に関係の深い国々の各法執行機関と効果的な情報交換を実施するとともに、G7、ICPO等のサイバー犯罪対策に係る国際的な枠組みへの積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の主催等を通じた多国間における協力関係の構築を推進する。また、外国法執行機関等に派遣した職員を通じ、当該機関等との連携強化を推進する。さらに、証拠の収集等のため外国法執行機関からの協力を得る必要がある場合について、外国の法執行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。

(エ)外務省において、我が国が2012年７月にサイバー犯罪に関する条約を締結し、同年11月から我が国について同条約の効力が生じたことを受け、引き続きアジア地域初の締約国として同条約の普及等に積極的に参画する。

3.2. 我が国の防御力・抑止力・状況把握力の強化

(1) 国家の強靭性の確保

> ① 任務保証
> ・ 政府機関及び重要インフラ事業者等におけるサイバーセキュリティの確保の推進
> ・ 防衛省・自衛隊のサイバー攻撃対処を行う部隊の能力向上、自らの活動が依存するネットワーク・インフラの防護強化、自衛隊の任務保証に関連する主体との連携の深化
>
> （2018 年戦略より）

(ア)都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、以下の取組を実施することにより、緊急対処能力の向上を図る。

- 重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供や保有するシステムに対する脆弱性試験を実施する。
- 事案発生を想定した共同対処訓練を実施する。
- サイバーテロ対策協議会を通じて、参加事業者間の情報共有を実施する。

(イ)防衛省において、対処機関としてのサイバー攻撃対処能力向上のため、最新技術を活用して、サイバー防護分析装置、サイバー情報収集装置、各自衛隊の防護システムの機能の拡充を図るとともに、多様な事態において指揮命令の迅速かつ確実な伝達を確保するため、防衛情報通信基盤（DII）のクローズ系及びネットワーク監視器材へ常続監視等を強化するための最新技術を適用していく。

(ウ)防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための官民協力関係の深化に向けた取組を実施する。また、任務保証の観点から、防衛省・自衛隊の活動が依存するネットワーク・インフラの防護を引き続き強化するとともに、自衛隊の任務保証に関連する主体との連携を深化させていく。

(エ)防衛省・自衛隊が保有する情報通信ネットワーク等に対する侵入試験（ペネトレーションテスト）について、実施に向けた所要の準備を進める。

(オ)防衛省において、サイバー攻撃等によって防衛省・自衛隊の情報通信基盤の一部が損なわれた場合においても、運用継続を実現する研究を実施する。

(カ)防衛省において、移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究を実施する。

② 我が国の先端技術・防衛関連技術の防護
- 防衛産業において、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組の実施
- 国立研究開発法人や先端的な技術情報を保有する大学等における対策の促進

（2018 年戦略より）

(キ)防衛省において、サイバーセキュリティの更なる確保のため、調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行うとともに、引き続き調査研究等を通じて必要な関連規則等の整備を進める。

(ク)科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。
- 内閣官房において、先端的な技術を保有する国立研究開発法人が、自立的に情報セキュリティ対策を講じていくことができるよう国立研究開発法人相互の協力の枠組みを通じ取組を促す。
- 文部科学省において、先端的な技術情報を保有する大学等に対して、サイバー攻撃による当該情報の漏えいを防止するための取組を促すとともに、支援する。

③ サイバー空間を悪用したテロ組織の活動への対策
- サイバー空間におけるテロ組織の活動に関する情報の収集・分析の強化その他の必要な措置の実施

（2018 年戦略より）

(ケ)内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。

(コ)警察庁及び法務省において、サイバー空間におけるテロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする態勢を拡充し、人的情報やオープンソースの情報を幅広く収集する等により、攻撃主体・方法等に関する情報収集・分析を強化するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携を図る。

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応
・ 我が国の安全保障を脅かすようなサイバー空間における脅威への、同盟国・有志国と連携し、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用した対応
・ 法執行機関、自衛隊を始めとする関係機関の能力強化

（2018 年戦略より）

(ア)適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進する。

(イ)防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。その際、悪意ある主体によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる。

(ウ)警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進する。また、都道府県警察において、サイバー攻撃特別捜査隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進する。

② 信頼醸成措置
・ 偶発的、不必要な衝突を防ぐための、国際的な連絡体制の構築
・ 二国間・多国間協議における情報交換、政策対話等を通じた信頼醸成

（2018 年戦略より）

(エ)内閣官房、外務省及び関係府省庁において、サイバー攻撃を発端とした不測事態の発生を未然に防止するため、ARFや二国間協議等を通じて、脅威認識やサイバーセキュリティ戦略等の政策について共有し、国際的な連絡体制等を平素から構築する。

(オ)経済産業省において、JPCERT/CCを通じて、インシデント対応調整や脅威情報の共有に係るCSIRT間連携の窓口を運営するとともに、各国の窓口チームとの間のMOU/NDAに基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、JPCERT/CCのFIRST、IWWNやAPCERTにおける活動、及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じた各国CSIRTとJPCERT/CCとのインシデント対応に関する連携を行う。

(3) サイバー空間の状況把握の強化

① 関係機関の能力向上
・ 関係機関の情報収集・分析能力の質的・量的向上
・ 高度な分析能力を有する人材の育成・確保、サイバー攻撃を検知・調査・分析等するための技術の開発・活用
・ カウンターサイバーインテリジェンスに係る取組の推進

（2018 年戦略より）

(ア)内閣官房において、「カウンターインテリジェンス機能の強化に関する基本方針」に基づき、各府省庁と協力し、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集約・分析を行い各府省との共有化を図る。また、政府機関が保有する機密情報が保護されるよう適切な措置を実施する。

(イ)警察庁及び法務省において、サイバーインテリジェンス対策に資する取組を実施する。

(ウ)警察庁及び都道府県警察において、以下の取組を推進することによりサイバー空間の状況把握の強化を図る。

- 警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。(再掲)
- 警察庁及び都道府県警察において、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を図る。(再掲)
- 警察庁において、システムの脆弱性の調査等を目的とした不正なアクセスが国内外で多数確認されている背景を踏まえ、こうした攻撃の未然防止活動、有事の緊急対処に係る能力向上に資する訓練、サイバー空間に関する観測機能の強化等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。また、サイバー攻撃の実態解明に必要不可欠な不正プログラム等の解析を推進する。

(エ)警察庁において、警察部内の高度な専門性を有する人材等の確保・育成を図る方策を検討する。

(オ)経済産業省において、JPCERT/CCがインシデント対応支援活動等において解析したマルウェア検体及びその解析結果について、同様の情報を有する国内外の関係機関との適切な相互共有やインターネット定点観測システム（TSUBAME）の運用との連動等の有効活用やその高度化を進める。

(カ)防衛省において、高度なサイバー攻撃からの防護を目的として、引き続き、国内外におけるサイバー攻撃関連情報を収集・分析する体制を強化するとともに、必要な機材の拡充を実施する。

(キ)防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。

(ク)法務省において、人的情報収集・分析を強化するための高度な専門性を有する人材の確保・育成を図る方策を検討する。

② 脅威情報連携
- 同盟国・有志国との脅威情報共有の推進
- 政府内の脅威情報共有・連携体制の強化

（2018年戦略より）

(ケ)内閣官房及び外務省において、外国関係機関との情報交換等を緊密に行い、主要国のサイバ

一攻撃対処や国家の関与が疑われるようなサイバー攻撃の動向等の情報収集・分析に努める。

(コ)内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

(サ)警察庁及び法務省において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を継続的に実施する。

3.3. 国際協力・連携

- 国際場裡での我が国の立場を主張できる官民の人材を確保し、育成する。

(2018 年戦略より)

(ア)内閣官房及び関係府省庁において、各国機関との連携、国際会議への参加、我が国での国際会議の開催等を通じ、我が国のサイバーセキュリティ人材が海外の優秀な技術者等と切磋琢磨しながら研鑽を積む場を増やす。

(1) 知見の共有・政策調整

- サイバーセキュリティに関する二国間の協議や国際会議を通じた、互いのサイバーセキュリティ政策や戦略、体制の情報交換の実施
- 戦略的パートナー国とのサイバーセキュリティ施策に関する協力・連携の強化

(2018 年戦略より)

(ア)内閣官房、総務省、外務省及び経済産業省において、日ASEANサイバーセキュリティ政策会議、二国間協議等の枠組みを通じ、アジア大洋州各国とのサイバー政策における相互理解と連携を強化する。また、総務省において、ワークショップの開催等を通じて、我が国とASEAN加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進する。

(イ)警察庁、法務省及び外務省において、国境を越えるサイバー犯罪の脅威に対抗するため、特にアジア太平洋地域諸国におけるサイバー犯罪対策に関する刑事司法制度の整備等が進むよう、二国間又は多国間の枠組みを活用した技術援助活動を積極的に推進する。

(ウ)防衛省及び関係府省庁において、東南アジア各国との間で、防衛当局間のITフォーラム等の取組を通じ、サイバー分野での連携やこれらの国に対する能力構築への協力、情報の収集や発信を推進していく。また、防衛省において、諸外国とのサイバー防衛協力を推進していく。

(エ)経済産業省において、アジアでの更なる情報セキュリティ人材の育成を図るため、アジア11か国・地域と相互・認証を行っている「情報処理技術者試験」について、我が国の情報処理技術者試験制度を移入して試験制度を創設した国（フィリピン、ベトナム、タイ、ミャンマー、モンゴル、バングラデシュ）が協力して試験を実施するための協議会であるITPECがアジア統一試験を実施しているところ、ITPECの更なる定着を図る。

(オ)内閣官房、外務省及び関係府省庁において、日米サイバー対話等の枠組みを通じ、幅広い分野における日米協力について議論し、両国間の政策面での協調や体制及び能力の強化、インシデント情報の交換等を推進し、同盟国である米国とのサイバー空間に関する幅広い連携を強化する。

(カ)総務省、外務省及び関係府省庁において、米国とのインターネットエコノミーに関する日米政策協力対話にて一致した、産業界及び他の関係者と共同してサイバーセキュリティ上の課題に取り組むことが不可欠であるとの認識に基づき、引き続き米国との情報共有を強化する。また、関連して、総務省において、日米の通信分野のISAC間の連携を推進する。

(キ)経済産業省において、国際協力体制を確立するという観点から、米NIST等の各国のサイバーセキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取組む。

(ク)防衛省において、日米サイバー防衛政策ワーキンググループ（CDPWG）の開催等を通じて、情報共有、訓練・人材育成等の様々な協力分野において日米サイバー防衛の連携を深めていく。また、新たな日米防衛協力のための指針で示された方向性に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を深化させていく。

(ケ)内閣官房、外務省及び関係府省庁において、二国間協議の枠組みを通じ、欧州各国との連携を強化する。防衛省において、日英防衛当局間サイバー協議、日NATOサイバー防衛スタッフトークスやNATO主催の演習への参加等を通じ、欧州各国とのサイバー防衛協力を引き続き推進していく。

(コ)内閣官房、外務省及び関係府省庁において、国際的な会議の場等を活用し、二国間協議に加え，各国とのサイバーセキュリティ分野における関係を強化する。

(サ)警察庁において、サイバー攻撃対策を推進するため、情報交換等国際的な連携を通じて、諸外国関係機関との連携強化を推進する。

(シ)経済産業省において、IPAを通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行うため、JIWG及びその傘下のJHAS、JEDSと定期的に協議を行う。

(ス)防衛省において、国家の関与が疑われるような高度なサイバー攻撃に対処するため、防衛省・自衛隊のサイバーセキュリティに係る諸外国との技術面・運用面の協力を推進する。

(2) 事故対応等に係る国際連携の強化

- CERT 間連携の強化
- 国際サイバー演習への参加、共同訓練等を通じた連携対処能力の向上

（2018 年戦略より）

(ア)内閣官房及び関係府省庁において、二国間協議、IWWN、日ASEANサイバーセキュリティ政策会議等のサイバー空間に関する多国間の情報共有枠組み等に参画し、それぞれの取組においてインシデント対応演習や机上演習等を通じて、各国との情報共有・インシデント発生時の国外との情報連絡体制を整備する。

(イ)経済産業省において、JPCERT/CCを通じ、各国のCSIRT連携による対応・対策を強化するため、サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組み（サイバーグリーン）の検討や、効率的な対処のためのオペレーション連携を実現するための基盤構築に資する開発、運用協力体制の検討を進める。

(ウ)経済産業省において、JPCERT/CCを通じて、主にアジア太平洋地域等を対象としたインターネット定点観測システム（TSUBAME）に関し、運用主体のJPCERT/CCと各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。また、アジア太平洋地域以外への観測点の拡大を進める。

(エ)経済産業省において、JPCERT/CC を通じて、以下の取組を行う。

- アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担うCSIRTの構築及び運用、連携の支援。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習の実施。
- アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施。
- 我が国企業が組込みソフトウェア等の開発をアウトソーシングしているアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施。

(3) 能力構築支援

- 様々な政策手段を活用した開発途上国における能力構築支援の実施

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、ASEAN 加盟国をはじめとする各国における能力構築支援に積極的に取り組む。取組に際しては、内閣官房を中心に、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2016 年 10 月）を踏まえ、政府及び関係機関が一体となって対応していく。

- 内閣官房において、日・ASEANサイバーセキュリティ政策会議を通じたセキュリティ人材育成の取組や一般向け意識啓発の取組を通じて、ASEAN加盟国の能力構築に貢献する。
- 警察庁において、アジア大洋州地域サイバー犯罪捜査技術会議やJICA課題別研修（サイバー犯罪対処能力向上）、JICA国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）の開催等を通じ、アジア大洋州地域をはじめとする各国における能力構築に貢献する。
- 総務省において、日ASEAN情報通信大臣会合を通じて、情報通信分野に関してASEAN域内各国・地域との間でのネットワークセキュリティ分野における能力構築等の連携を推進する。また、APT（アジア・太平洋電気通信共同体）における取組やITU-D等の取組を通じて、研修やセミナーを開催することにより、諸外国に対する意識啓発に取り組む。
- 外務省において、警察庁等とも協力しつつ、第３回日・ASEANサイバー犯罪対策対話や日ASEAN統合基金の活用，UNODCプロジェクトへの拠出を通じて、ASEAN加盟国のサイバー犯罪対策能力構築支援を行う。その他国際機関などと連携したプロジェクトについても検討する。
- 経済産業省において、ASEAN加盟国に対し、ISMS、CSMSに関する研修・セミナー等を通じて、我が国のセキュリティマネジメントに関するノウハウを共有することで、ASEAN加盟国への能力構築支援へ貢献する。
- 経済産業省において、JPCERT/CCを通じ、アジア太平洋地域、アフリカ等において、各国

における対外・対内調整を担うCSIRTの構築及び運用、連携の支援を行う。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習実施を行う。また、アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施等の活動等を行う。さらに、我が国企業が組込みソフトウェア等の開発をアウトソーシングしている先のアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。

(イ)経済産業省及び IPA 産業サイバーセキュリティセンター（ICSCoE）が米国土安全保障省及び同省傘下の ICS-CERT と協力し、ASEAN をはじめとしたアジア太平洋地域の国々に対する産業サイバーセキュリティの共同演習実施を通じた能力構築支援を開始する。

4. 横断的施策

4.1. 人材育成・確保

・ 人材の需要と供給を相応するための好循環を形成するため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化

（2018 年戦略より）

(ア)内閣官房において、関係府省庁と連携しつつ、「サイバーセキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成取組方針」に基づき、普及啓発・人材育成専門調査会等を通じて、施策間連携を図りつつ、関係施策を促進していく。

(イ)内閣官房において、「サイバーセキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成取組方針」を踏まえ、さまざまな人材育成施策について、施策間の連携を強化するとともに、横断的かつ継続的に人材育成施策の全体像が把握できるよう、「見える化」の推進を図る。

(1) 戦略マネジメント層の育成・定着

・ 「戦略マネジメント層」に関する経営層の理解の促進と産業界と連携したその定着
・ 戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進

（2018 年戦略より）

(ア)経済産業省において、IPAに設置した「産業サイバーセキュリティセンター」において、ITとOT双方のスキルを核とした上でビジネススキルやマネジメントスキル・リーダーシップをバランスよく兼ね備えた、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。また、重要インフラ等における実際の制御システム等の安全性・信頼性を検証する事業も実施し、対策強化に繋げる。

(イ)経済産業省において、IPAの「産業サイバーセキュリティセンター」を通じ、高度な経営判断を補佐する戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングを行うプログラムを2018年秋から開始する。

(ウ)経済産業省において、セキュリティ教育を提供するため、教える側の質的向上・量的拡充のため、「学」の教員向けにIPA、JPCERT/CCにより、FD（Faculty Development）等の研修機会の提供を実施していく。

(エ)文部科学省において、IT技術者等のサイバーセキュリティに係る素養の向上を図るため、高等教育機関等における社会人学生の受け入れを促進する。

(オ)内閣官房において、戦略マネジメント層を担う人材の育成に向けて、必要な知識・スキルを身に着けるための試行的取組について検討する。

(2) 実務者層・技術者層の育成

・ 学び直しによるスキルの開発や実践的な演習

（2018 年戦略より）

(ア)警察庁において、国立高等専門学校機構と連携し、高等専門学校へのサイバーセキュリティ講義を実施することで、学生のサイバーセキュリティ分野に対する興味・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上を図る。

(イ)都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を図る。（再掲）

(ウ)総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。

(エ)文部科学省において、高等専門学校におけるセキュリティ教育の強化のための施策として、企業等のニーズを踏まえた技術者のセキュリティ教育に必要な教材・教育プログラム開発を進める。また、並行して、2016年より、段階的に整備を進めてきた情報セキュリティ教育の演習拠点（10拠点）については、日々進歩しているサイバー攻撃技術に対応するため、定期的な環境更新（アップデート）を進めるなど、全国の高等専門学校生が共同で利用できるサイバーレンジ（実践的な演習環境）の提供に向けた取組を推進する。

(オ)厚生労働省において、離職者や在職者を対象として職業に必要な技能及び知識を習得させるため、サイバーセキュリティに関する内容を含む公共職業訓練を実施するとともに、離職者や在職者を対象とした教育訓練給付制度において、サイバーセキュリティに関する内容を含む教育訓練を指定する。

(カ)経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として2016年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施と当該制度の普及のため、企業や団体への周知等を積極的に行う。

(キ)経済産業省において、国家試験である情報処理技術者試験において、組織のセキュリティポリシーの運用等に必要となる知識を問う「情報セキュリティマネジメント試験」の普及を図る。

(ク)内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る。

(ケ)経済産業省において、IPAを通じ、各府省庁、全国各地の関係団体と協力し、インターネットを利用する一般の利用者を対象としてSNSの安全な利用方法を含む情報セキュリティに関する啓発を行うインターネット安全教室を引き続き開催していく。

・ 突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成

（2018 年戦略より）

(コ)経済産業省において、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的としてIPAと「セキュリティ・キャンプ協議会」にて共催しているセキュリティ・キャンプについて、サイバーセキュリティを取り巻く状況の変化への更なる対応を図る。

(サ)経済産業省において、ITを駆使してイノベーションを創出することのできる独創的なアイディア・技術を有する人材の発掘・育成に向け、「未踏IT人材発掘・育成事業」を実施する。

(シ)経済産業省において、情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF」について、NPO日本ネットワークセキュリティ協会及び企業が共同で開催地域拡大や競技内容の向上を図り、更なる人材候補者を増やすべく、大学等との連携や多様なコンテストの在り方を検討するとともに、同協会で実施するコンテスト（「SECCON 2018」）について普及・広報の支援を行う。

(ス)防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。

(セ)防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。

(ソ)防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための具体的・実効的連携を深化するための取組を実施する。

(3) 人材育成基盤の整備

・ 知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討
・ 教育課程内での情報活用能力の育成、情報モラル教育
・ 教員の研修の充実
・ 自由にサイバー関連ツール､機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備
・ 大学・高等専門学校等の高等教育段階における情報技術人材の育成

（2018 年戦略より）

(ア)経済産業省において、情報サービスの提供に必要な実務能力を明確化、体系化した共通指標であるITスキル標準の全面的な改訂に向け、第４次産業革命に伴い主流となる新技術に対応するIT人材に焦点を当てたスキル標準の検討を引き続き行う。

(イ)文部科学省において、新学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する。特に、各学校における指導の改善・充実に向けて、教科等横断的な情報活用

能力の育成に係るカリキュラム・マネジメントの在り方や、それに基づく指導方法・教材の利活用等について、実践的な研究を実施する。

(ウ)文部科学省において、2016年11月の教育職員免許法改正及び2017年11月の同法施行規則改正に基づき、ICTを用いて効果的な授業を行ったり、適切なデジタル教材を開発・活用したりすることができる力を教師を志す学生に身に付けさせるため、各教科の指導法を学ぶ科目について、当該教科の特性に応じた情報機器や教材の効果的な活用方法を新たに内容に加えた教員養成課程の審査を行う。

(エ)文部科学省において、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。

(オ)文部科学省において、動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、教員等を対象としたセミナーを実施する。

(カ)総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」における「SecHack365」の取組を通じて、若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導し、セキュリティイノベーターの育成に取り組む。

(キ)文部科学省において、複数の大学や産学の連携によるサイバーセキュリティに係る実践的な教育ネットワークの構築やPBL（課題解決型学習）の実施を支援する。

(ク)文部科学省及び経済産業省において、高度なITの知識と経営などその他の領域における専門知識を併せもつハイブリッド型人材の育成を進める。

(4) 各府省庁におけるセキュリティ人材の確保・育成の強化

- 各府省庁におけるセキュリティ人材の着実な確保・育成を継続
- 毎年度、計画の見直しを行い、一層の取組の強化

（2018 年戦略より）

(ア)各府省庁において、内閣官房の主導によりPDCAサイクルを更に充実させることにより、「サイバーセキュリティ人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT人材確保・育成計画」の見直しを行い、体制の整備・人材の拡充、有為な人材の確保、一定の専門性を有する人材の育成や適切な処遇の確保を含む政府部内のセキュリティ人材の充実に係る諸施策をより一層推進する。

(イ)各府省庁において、2020年東京オリンピック・パラリンピック競技大会の成功等に向けて、サイバーセキュリティ・情報化審議官等が中心となって、「各府省庁セキュリティ・IT人材確保・育成計画」に沿って引き続き体制の整備と適切な処遇の確保に取り組む。

(ウ)各府省庁のセキュリティ・IT人材を育成・確保するため、内閣官房及び総務省において、情報システム統一研修等各コースの内容の更なる充実に向けた取組を進めるとともに、2018年１月に策定された「橋渡し人材のスキル認定の基準」に基づく橋渡し人材（部内育成の専門人材）のスキル認定が推進されるよう、各府省庁に対する支援等を行う。

(エ)内閣官房において、サイバーセキュリティ・情報化審議官等の研修等を通じて政府機関内における相互の事例共有、意見交換等の継続的な実施を促進する。また、府省庁を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会を開催する。

(5) 国際連携の推進

- 国際的な基準を踏まえた人材育成プログラムの認定など海外組織との間での連携を促すための仕組み作り
- 海外におけるサイバーセキュリティ人材の能力構築への貢献

（2018 年戦略より）

(ア)内閣官房において、主要国における取組について調査の上、人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討を行う。

(イ)経済産業省において、今後、ますますの経済連携が求められるASEAN各国において、我が国企業が安全に活動でき、また、我が国の持つノウハウをASEAN諸国と共有できるよう、セキュリティマネジメント導入のためのノウハウ支援等を行う。

4.2. 研究開発の推進

(1) 実践的な研究開発の推進

- 先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発

（2018 年戦略より）

(ア)総務省において、NICTを通じ、巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、サイバー攻撃観測技術の高度化、機械学習等を応用した通信分析技術やマルウェア自動分析技術の高度化等のアドバンスト・サイバーセキュリティ技術の研究開発を行う。

(イ)文部科学省において、サイバーセキュリティを含む経済・社会的な重要課題を解決につなげることが期待される、量子コンピュータをはじめとした量子科学技術に関する研究開発を推進する。

(ウ)文部科学省において、理化学研究所革新知能統合研究センター（AIPセンター）を通じ、革新的な人工知能基盤技術の構築と、サイバーセキュリティを含む社会的課題の解決に向けた応用研究等を進めていく。あわせて、JSTの戦略的創造研究推進事業において、サイバーセキュリティを含めた研究課題を支援する。

(エ)経済産業省において、AIST等を通じ、IoTシステムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、などを両立させるための革新的、先端的技術の基礎研究に取り組む。

(オ)経済産業省において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバ

一空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるコア技術の調査・研究開発・実証等を行う。

- サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発
- 機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発
- 不正なプログラムや回路が仕込まれていないことの検証を行うための体制の整備とそのための研究開発

（2018 年戦略より）

(カ)経済産業省において、制御システムの挙動を解析し、サイバー攻撃を検知・予測する技術開発や、可用性を確保した脆弱性への対処技術に関する研究を行う。

(キ)内閣府において、関係府省庁と連携して、戦略的イノベーション創造プログラム（SIP）第1期「重要インフラ等におけるサイバーセキュリティの確保」により、2020年東京オリンピック・パラリンピック競技大会を支える重要インフラに導入して有効性を実証し、将来の国内インフラ産業の安定運用やインフラ輸出に貢献するための研究開発・社会実装を行う。本プロジェクトでは、制御・通信機器のセキュリティ確認（機器やソフトウェアの真正性・完全性を確かめること）技術、動作監視・解析技術、異常検知時に制御システムの可用性を重視する防御技術等を開発する。

(ク)内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、中小企業を含むサプライチェーン全体を守ることに活用できる、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進する。本プロジェクトでは、IoT機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。また、本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。(再掲)

(ケ)総務省において、スマートシティにおけるプラットフォームに係るセキュリティ要件の具体化や所用の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を進める。

(コ)総務省において、戦略的情報通信研究開発推進事業（SCOPE）のなかで、IoT機器などのハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を実施する。

(サ)内閣官房において、関係府省と連携しつつ、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、不正なプログラムや回路が仕込まれていないことの技術的検証等を行うための体制整備を図るとともに、そのために必要となる研究開発について関係施策を促進していく。

・ 政府機関や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃活動を把握、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進

（2018 年戦略より）

(シ)総務省において、NICTを通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図り、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を行う。また、サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とするサイバーセキュリティ・ユニバーサル・リポジトリ（CURE）を構築するとともに、CUREに基づく自動対策技術の確立等を行う。

(ス)総務省において、脆弱なIoT機器のセキュリティ対策のため、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンのための研究開発を行う。

・ 計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術の研究開発
・ サイバーセキュリティ対策における制度上の課題に関する調査・研究

（2018 年戦略より）

(セ)内閣府において、革新的研究開発推進プログラム(ImPACT)「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」により、機密情報を安全に伝送・保管できる通信ネットワークの構築を目指して量子暗号技術の研究開発を行う。

(ソ)総務省において、NICTを通じ、情報理論的安全性（暗号が情報理論的な意味で無条件に安全である性質）を具備した量子暗号等を活用した量子情報通信ネットワーク技術の確立に向け、研究開発を実施する。

(タ)総務省において、盗聴や改ざんが極めて困難な量子暗号通信を、超小型衛星に活用するための技術の確立に向け、研究開発を実施する。

(チ)内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。(再掲)

(ツ)総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、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、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。(再掲)

・ サイバーセキュリティの研究開発の成果の普及や社会実装の推進、海外のイベント等への積極的な参加等を通じた、国際的な情報発信、共同研究の実施や研究成果の国際標準化等の研究開発に係る官民の国際連携の強化

（2018 年戦略より）

(テ)総務省及び経済産業省において、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC1/SC27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進する。(再掲)

(ト)総務省において、サイバーセキュリティ関連産業の国際展開及びサイバーセキュリティ関連の研究開発の国際的な発信等のため、我が国の関係組織の主要な国際展示会への出展に資する事業を実施する。

(ナ)経済産業省において、IPAを通じ、情報セキュリティ分野と関連の深い国際標準化活動であるISO/IEC JTC1/SC27が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。

(2) 中長期的な技術・社会の進化を視野に入れた対応

- 人文社会学的視点も含めた様々な領域の研究との連携、融合領域の研究を促進

(2018 年戦略より)

(ア)内閣官房において、各府省庁と連携し、信頼性工学、心理学等の様々な社会科学的視点も含めて策定した「サイバーセキュリティ研究開発戦略」について、目下の課題を解決すべく、融合領域の研究動向についての調査等を検討する。

4.3. 全員参加による協働

- サイバーセキュリティの普及啓発に向けた総合的な戦略及び具体的なアクションプランの策定

(2018 年戦略より)

(ア)内閣官房において、「新・情報セキュリティ普及啓発プログラム」の改訂を行い、普及啓発施策の方向性と具体的な行動計画をとりまとめる。

- 必要な情報発信や国民からの相談対応
- 産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、関係者による実践を推進

(2018 年戦略より)

(イ)内閣官房において、家庭や教育現場、企業内等でのセキュリティ意識向上のため、緊急時における注意・警戒情報やサイバーセキュリティに関する役立ち情報等について、SNS等を用いた発信を引き続き行うとともに、より効果的な手段について検討を行う。

(ウ)経済産業省において、IPAを通じ、「情報セキュリティ安心相談窓口」、さらに、高度なサイバー攻撃を受けた際の「標的型サイバー攻撃の特別相談窓口」によって、サイバーセキュリティ対策の相談を受け付ける体制を充実させ、一般国民や中小企業等の十分な対策を講じることが困難な組織の取組を支援する。

(エ)内閣官房において、主体的に普及啓発活動を行う動きが地域レベルでも促進されるよう、「情報セキュリティ社会推進協議会」等を活用しつつ、産学官民の連携・協力を通じて、必要な取組について検討を進める。

(オ)総務省、法務省及び経済産業省において、電子署名などのトラストサービスの利活用等に関するセミナーの開催及びHPを活用した情報提供を行うことで、国民による安全なサイバー空間の利用をサポートするとともに、認定認証事業者に対する説明会の開催、民間事業者等からの電子署名に関する相談対応等を行うことで、企業における電子署名の利活用の普及促進策を検討・実施する。

(カ)経済産業省において、IPA、JPCERT/CCを通じて、情報漏えいの新たな手法や手口の情報収集に努め、一般国民や中小企業等に対し、ウェブサイトやメーリングリスト等を通じて対策情報等、必要な情報提供を行う。

(キ)経済産業省において、IPAを通じ、広く企業及び国民一般に情報セキュリティ対策を普及するため、地域で開催されるセミナーや各種イベントへの出展、普及啓発資料の配布、セキュリティプレゼンター制度の運用などにより情報の周知を行い、セキュリティ啓発サイトや各種ツール類を用いて、対策情報の提供を行う。

- 「サイバーセキュリティ月間」のさらなる充実

（2018 年戦略より）

(ク)内閣官房において、行動計画に基づき、NISCが中核的役割を担いつつ、各府省庁や民間の取組主体と協力して、「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催や情報発信等を通じ普及啓発活動を進める。

- 国民向けのわかりやすい解説書の作成・普及
- 学校教育を通じた、情報モラル教育の一部としてのサイバーセキュリティ教育の推進

（2018 年戦略より）

(ケ)内閣官房において、サイバーセキュリティに関する基本的な知識を紹介したハンドブックについて、引き続き内容の見直しを行うとともに、普及及び活用を促す取組を行う。

(コ)経済産業省において、個人情報も含む情報漏えい対策に取り組むため、IPAを通じ、ファイル共有ソフトによる情報漏えいを防止する等の機能を有する「情報漏えい対策ツール」を民間の配布サイトも活用して一般国民に提供する。

(サ)総務省において、文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るため、多くの青少年が初めてスマートフォン等を手にする春の卒業・進学・新入学の時期に特に重点を置き、関係府省庁と協力して啓発活動を集中的に展開する「春のあんしんネット・新学期一斉行動」の取組や、「e-ネットキャラバン」等の青少年や保護者等に向けた啓発講座の実施等を行う。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。

(シ)文部科学省において、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルールづくりの重要性の普及啓発を実施する。

(ス)文部科学省において、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。(再掲)

(セ)文部科学省において、動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、教員等を対象としたセミナーを実施する。(再掲)

(ソ)経済産業省において、IPAを通じ、各府省庁と協力し、情報モラル/セキュリティの大切さを児童・生徒が自身で考えるきっかけとなるように、IPA主催の標語・ポスター・４コマ漫画等の募集及び入選作品公表を行い、国内の若年層における情報モラル/セキュリティ意識の醸成と向上を図る。

(タ)経済産業省において、IPAを通じ、各府省庁と協力し、家庭や学校からインターネットを利用する一般の利用者を対象として情報セキュリティに関する啓発を行う安全教室について、全国各地の関係団体と連携し引き続き開催していく。

・ 利用者がサイバーセキュリティの取組を適切に実施できるよう事業者や関係団体等の取組が促進される環境の整備、サイバーセキュリティの確保に資するガイドラインの整備とその着実な実施を推進

(2018 年戦略より)

(チ)総務省において、安全に無線LANを利用できる環境の整備に向けて、引き続き利用者・提供者において必要となるセキュリティ対策に関する検討を行うとともに、利用者・提供者に対する周知啓発を実施する。特に、セキュアな公衆無線LAN環境の実現に向けて、各種ガイドラインの改定や教育コンテンツを活用した周知・啓発、データ利活用施策との連携、セキュアな公衆無線LAN環境の優良事例の調査・整理及びこれを踏まえた所要の政策支援等の取組を行う。

(ツ)経済産業省において、IPAを通じて、サイバーセキュリティに関する現状把握及び対策を実施する際の参考となる最新の動向の収集・分析・報告書の公表等により、サイバー空間利用者への啓発を推進する。

5. 推進体制

(ア) 内閣官房において、関係機関の一層の能力強化に向けて、JPCERT/CCと締結した国際連携活動及び情報共有等に関するパートナーシップの一層の深化を図るため、2015年度に構築した情報共有システムの機能向上を図るとともに連携体制についても逐次見直しを実施する。また、総合的分析機能の強化を図る。さらに、NICTと締結した研究開発や技術協力等に関するパートナーシップに基づいてNICTとの協力体制を整備し、サイバーセキュリティ対策に係る技術面の強化を図る。

(イ) 内閣官房において、2018年戦略に基づく諸施策が着実に実施されるようにするとともに、全ての主体によるサイバーセキュリティに関する自律的な取組を促進するため、各種イベント等における説明会の開催などを通じて、国内外の関係者への2018年戦略の発信を積極的に行い、周知を図る。

(ウ) 内閣官房において、国民の生命等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（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、関係府省庁、重要インフラ事業者等と連携した初動対処訓練を実施する。（再掲）

(エ) 内閣官房において、「2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」（2017年3月21日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。具体的には、オリパラ競技大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象として、リスク評価に基づく対策の促進と、情報の共有、インシデント発生時の調整役となるための組織であるサイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の整備を推進する。2018年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。また、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）については、2018年度末を目途に構築し、2019年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。（再掲）

参考１　用語解説

	用　　語	解　　説
A	AIST	national institute of Advanced Industrial Science and Technologyの略。国立研究開発法人産業技術総合研究所（産総研）。2001年１月６日の中央省庁再編に伴い、通商産業省工業技術院及び全国15研究所群を統合再編し、通商産業省及びその後継の経済産業省から分離して発足した独立行政法人。
	APCERT	Asia Pacific Computer Emergency Response Teamの略。各国・地域におけるCSIRTの活動と連携し、アジア太平洋地域におけるコーディネーションの実施等を行う。
	AppGoat	IPAが無償提供する脆弱性体験学習ツール。学習教材と演習環境がセットになっており、脆弱性の検証手法から原理、影響、対策までを演習しながら学習できる。
	APT	Asia-Pacific Telecommunityの略。アジア太平洋電気通信共同体。アジア・太平洋地域の電気通信の開発促進及び地域電気通信網の整備・拡充を目的として1979年に設立。
	ARF	ASEAN Regional Forumの略。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。
	ASEAN	Association of South East Asian Nationsの略。東南アジア諸国連合。
B	BCP	Business Continuity Planの略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCPのうち情報（通信）システムについて記載を詳細化したものがIT-BCP（ICT-BCP）である。
C	CC	Common Criteriaの略。ISO/IEC 15408のこと。情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
	CCRA	Common Criteria Recognition Arrangementの略。CCに基づいたセキュリティ評価・認証の相互承認に関する協定。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005年以降順次構築が進められ、2017年３月末現在、13分野で18セプターが活動。
	CERT/CC	Computer Emergency Response Team/Coordination Centerの略（サートシーシー）。サイバー攻撃情報やシステムの脆弱性関連情報を収集・分析し、関係機関に情報提供等を行っている非営利団体の一般的な名称。複数の国で設立されており、日本にはJPCERT/CCが設置されている。
	CISO	Chief Information Security Officerの略。最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣サイバーセキュリティセンター長である。
	CRYPTREC	Cryptography Research and Evaluation Committeesの略。電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及びIPAが共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。
	CSIRT	Computer Security Incident Response Teamの略（シーサート）。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のこと。
	CSMS	Cyber Security Management Systemの略。制御システムのセキュリティマネジメントシステム。
	CTF	Capture The Flagの略。情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト。
	CURE	国立研究開発法人情報通信研究機構（NICT）において研究開発している、サイバーセキュリティ研究及びセキュリティ・オペレーションの遂行に不可欠な各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等のサイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする仕組み。
	CVSS	Common Vulnerability Scoring Systemの略。情報システムの脆弱性の深刻度に対するオープンで汎用的な評価手法。

	CYMAT	CYber incident Mobile Assistance Teamの略（サイマット）。我が国の機関等において大規模なサイバー攻撃等により政府として一体となって迅速・的確に対応すべき事態等が発生した際に、機関の壁を越えて連携し、被害拡大防止等について機動的な支援を行うため、2012年６月に内閣官房に設置した体制のこと。
D	DII	Defense Information Infrastructureの略。防衛省の基盤的共通通信ネットワーク。
	DKIM	Domain Keys Identified Mailの略。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールへの対策の一つとして利用可能。
	DMARC	Domain-based Message Authentication, Reporting &Conformanceの略。電子メールにおける送信ドメイン認証技術の一つであり、SPF・DKIMのドメイン認証技術を利用し、メールの正当性を送信者と受信者間で確認する仕組み。
E	eラーニング	electronic learningの略。情報通信技術を用いた教育、学習のこと。
F	FIRST	Forum of Incident Response and Security Teamsの略。各国のCSIRTの協力体制を構築する目的で、1990年に設立された国際協議会であり、2017年５月現在、世界80ヶ国の官・民・大学等369の組織が参加している。
G	G7	Group of Seven（主要７か国首脳会議）の略。
	GSOC	Government Security Operation Coordination teamの略（ジーソック）。政府機関情報セキュリティ横断監視・即応調整チーム。政府機関等に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うためのGSOCシステムを運用する体制のこと。内閣官房内閣サイバーセキュリティセンターにおいて、2008年４月から運用開始。 　近年のサイバー攻撃の複雑・巧妙化を踏まえ、2017年４月に運用開始した第３期GSOCでは、検知・解析機能の強化、センサーの増強等を図っている。また、2017年４月からは、独立行政法人等に対する監視体制（第二GSOC）の運用を開始し、従前からの政府機関に対する監視体制（第一GSOC）と連携を図り、監視体制を強化している。
I	icat	IPAの運営するサイバーセキュリティ注意喚起サービス。ソフトウェア等の脆弱性に関する情報をタイムリーに発信する。
	ICPO	International Criminal Police Organizationの略（インターポール）。国際刑事警察機構。
	ICT	Information and Communications Technologyの略。情報通信技術のこと。
	IoT	Internet of Thingsの略。あらゆる物がインターネットを通じて繋がることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。従来のパソコン、サーバ、携帯電話、スマートフォンのほか、ICタグ、ユビキタス、組込システム、各種センサーや送受信装置等が相互に情報をやり取りできるようになり、新たなネットワーク社会が実現すると期待されている。
	IoT推進コンソーシアム	IoT推進に関する技術の開発・実証や新たなビジネスモデルの創出を推進するための体制を構築することを目的として、2015年10月に設立された産官学が参画・連携する組織。
	IoTセキュリティガイドライン	IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、2016年７月に策定。IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その関係者がセキュリティ確保の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ、明確化することによって、産業界による積極的な開発等の取組を促すとともに、利用者が安心してIoT機器やシステム、サービスを利用できる環境を生み出すことにつなげるもの。
	IPA	Information-technology Promotion Agencyの略。独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	ISAC	Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMS	Information Security Management Systemの略。情報セキュリティマネジメントシステム。
	ISO	International Organization for Standardizationの略。電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う国際標準化機関。

	ISO/IEC JTC1 SC27	セキュリティコントロールとサービスの分野を対象に、国際規格を策定するISO/IEC JTC1配下の分科委員会。
	ISO/IEC JTC1 SC41	インターネット・オブ・シングスと関連技術の分野を対象に、国際規格を策定するISO/IEC JTC1配下の分科委員会。
	ISP	Internet Service Providerの略。インターネット接続事業者。
	ITPEC	IT Professionals Examination Councilの略。アジア統一共通試験実施委員会。我が国の情報処理技術者試験制度を移入して試験制度を創設した国（６カ国）が協力して試験を実施するための協議会。
	ITU	International Telecommunication Unionの略。国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-D	International Telecommunication Union Telecommunication Development Sectorの略。ITUの電気通信開発部門。
	ITU-T	International Telecommunication Union Telecommunication Standardization Sectorの略。ITUの電気通信標準化部門。
	IT製品の調達におけるセキュリティ要件リスト	経済産業省及びIPAの共同により、2014年５月に策定。安全性・信頼性の高いIT製品等の利用推進の取組の一つとして、従来の「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」を改訂したもの。
	ITセキュリティ評価及び認証制度	IT製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、情報セキュリティの国際標準ISO/IEC 15408に基づいて第三者が評価し、結果を公的に検証し、原則公開する制度。
	IWWN	International Watch and Warning Networkの略。サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
J	JC3	Japan Cybercrime Control Centerの略。一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTAとして設立された。
	JCMVP	Japan Cryptographic Module Validation Programの略。「暗号モジュール試験及び認証制度」を参照。
	J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japanの略。サイバー情報共有イニシアティブ。IPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。
	JHAS	Joint Interpretation Library（JIL）Hardware-related Attacks SWGの略。欧州の認証機関、評価機関、スマートカードベンダ、ユーザーなどからなる作業部会。
	JISEC	Japan Information Technology Security Evaluation and Certification Schemeの略。ITセキュリティ評価及び認証制度を参照。
	JIWG	Joint Interpretation Library（JIL）WGの略。欧州における、スマートカードなどのセキュリティ認証機関からなる技術ワーキンググループ。
	JPCERT/CC	Japan Computer Emergency Response Team/Coordination Centerの略。インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生の状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている機関。特定の政府機関や企業からは独立した組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。 1996年10月に「コンピュータ緊急対応センター」として発足。
	JVN	Japan Vulnerability Notesの略。JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイト。
	JVNiPedia	IPAが運営する脆弱性情報データベース。
L	LAN	Local Area Networkの略。企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。
	LGWAN	Local Government Wide Area Networkの略。総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。

M	M2M	Machine-to-Machineの略。ネットワークに繋がれた機器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のこと。例としては、情報通信機器（情報家電、自動車、自動販売機等）や建築物等に設置された各種センサー・デバイスを、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、防災等の多様な分野のサービスを実現するなど。より広義の概念でIoT（Internet Of Things）と呼ばれることもある。
	MOU/NDA	Memorandum Of Understanding/Non-Disclosure Agreementの略。覚書及び秘密保持契約。
	MyJVN	JVNiPedia で配布されている脆弱性チェックツール。PCのソフトウェアが最新か、セキュリティ設定に問題がないか等を確認し、対策が必要な場合は情報へのリンクを提供する。
N	NATIONAL 318(CYBER) EKIDEN	府省庁職員を対象とした、１府12省庁対抗による競技形式のサイバー攻撃対処訓練のこと。
	NCFTA	National Cyber-Forensics and Training Allianceの略。FBI、民間企業、学術機関を構成員として米国に設立された米国の非営利団体。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。
	NICT	National Institute of Information and Communications Technologyの略。国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を実施するとともに、民間や大学が実施する情報通信分野の研究開発の支援の実施等を行う独立行政法人。
	NII	National Institute of Informaticsの略。国立情報学研究所。大学共同利用機関法人情報・システム研究機構の一員。情報学という新しい学問分野での「未来価値創成」を目指すわが国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	NISC	National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。
	NIST	National Institute of Standards and Technologyの略。アメリカ国立標準技術研究所。
O	OS	Operating Systemの略。多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。
P	PBL	Project Based Learningの略。課題解決型学習。
	PDCAサイクル	Plan-Do-Check-Act cycle。事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つ。Plan（計画）→Do（実行）→Check（評価）→Act（改善）の４段階を繰り返すことによって、業務を継続的に改善する。
	PP	Protection Profileの略。IT製品のセキュリティ上の課題に対する要件をCCに従って規定したセキュリティ要求仕様。主に調達要件として用いられる。
S	SCAP	Security Content Automation Protocol の略。情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様。
	SECCON 2018	SECCON：SECurity CONtest 2018の略。情報セキュリティをテーマに多様な競技を開催する情報セキュリティイベントの2018年における名称。競技を通じた実践的情報セキュリティ人材の発掘・育成、技術実践の場の提供を目的とする。
	SIP	cross-ministerial Strategic Innovation promotion Programの略。戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS	Social Networking Serviceの略。社会的ネットワークをインターネット上で構築するサービスのこと。友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、「友人の友人」といったつながりを通じて新たな人間関係を構築したりする場を提供する。

	SOC	Security Operation Centerの略。セキュリティサービス及びセキュリティ監視を提供するセンター。
	Society5.0	狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略2017（平成29年6月9日閣議決定））
	SPF	Sender Policy Frameworkの略。電子メールにおける送信ドメイン認証の一つ。差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる。
	STARDUST	国立研究開発法人情報通信研究機構（NICT）において研究開発している、高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能とするサイバー攻撃誘引基盤。
T	TSUBAME	JPCERT/CCが運営するインターネット定点観測システム。Internet上に観測用センサーを分散配置し、セキュリティ上の脅威となるトラフィックの観測を実施。得られた情報はウェブサイト等を通して提供されている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	安全なIoTシステムのためのセキュリティに関する一般的枠組	NISCにおいて、2016年８月に策定。従来の情報セキュリティの確保に加え、新たに安全確保が重要なIoTシステムは、セキュリティ・バイ・デザインの思想で設計、構築、運用されることが不可欠であるため、安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにしたもの。
い	イノベーション	新技術の発明や新規のアイデア等から、新しい価値を創造し、社会的変化をもたらす自発的な人・組織・社会での幅広い変革のこと。
	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
か	カウンターインテリジェンス	外国の敵意ある諜報活動に対抗する情報防衛活動のこと。
	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。
	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。
く	クラウドサービス	インターネット等のブロードバンド回線を経由して、データセンタに蓄積されたコンピュータ資源を役務（サービス）として、第三者（利用者）に対して遠隔地から提供するもの。なお、利用者は役務として提供されるコンピュータ資源がいずれの場所に存在しているか認知できない場合がある。
	クラウドサービス提供における情報セキュリティ対策ガイドライン	総務省において、2014年４月策定。2018年７月改定。クラウドサービス利用の進展状況等に対応するため、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関するガイドライン。
こ	高度サイバー攻撃対処のためのリスク評価等のガイドライン	2016年10月７日サイバーセキュリティ対策推進会議（CISO等連絡会議）決定。政府機関等におけ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及びサイバー攻撃への対処体制の充実・強化に資するために策定されたもの。
	コーポレート・ガバナンス・システム	会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組みに関するシステム。
	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	サイバーインテリジェンス	情報通信技術を用いた諜報活動のこと。
	サイバー攻撃特別捜査隊	サイバー攻撃対策の強化のため、14都道府県警察に設置。サイバー攻撃に関する情報収集、被害の未然防止及び犯罪捜査に専従している。
	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。

	サイバーセキュリティ経営ガイドライン	経済産業省及びIPAの共同により、2015年12月にVer1.0を策定。大企業および中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのガイドライン。
	サイバーセキュリティ月間	サイバーセキュリティについて国民に広く普及啓発するため、2009年より毎年２月に実施してきた「情報セキュリティ月間」を、2015年より、２月１日から３月18日（「サイバーの日」）までに期間を拡大したもの。月間の期間中、サイバーセキュリティについて、「知る・守る・続ける」をキャッチフレーズに、普及啓発に関する行事や関連キャンペーン等を行っている。
	サイバーセキュリティ研究開発戦略	情報通信技術の進化や、人間と情報の関わり方が変化していることを意識しつつ、近い将来及び中長期的な将来における、サイバーセキュリティ研究開発の方向性についてビジョンを提示した文書。
	サイバーセキュリティ人材育成プログラム	サイバーセキュリティ関連人材の育成の方向性を示した「サイバーセキュリティ人材育成プログラム」を2017年４月18日にサイバーセキュリティ戦略本部にて決定。
	サイバーセキュリティ戦略（2018年戦略）	我が国のサイバーセキュリティ政策に関する国家戦略であり、2015年９月４日に閣議決定された前戦略からのサイバー空間に係る現状認識を踏まえ、目指すサイバーセキュリティの基本的な在り方として、「持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進」を位置づけており、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるもの。
	サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。
	サイバーテロ対策協議会	警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する組織。全国の都道府県に設置されており、サイバー攻撃の脅威や情報セキュリティに関する情報共有のほか、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃対策セミナー等の実施により、重要インフラ事業者等のサイバーセキュリティや緊急対処能力の向上に努めている。
	サイバーフォースセンター	サイバー攻撃対策の技術的基盤として、警察庁情報通信局に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、事案発生時には技術的な緊急対処の拠点として機能する。
	サプライチェーン	取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。
	産業サイバーセキュリティ研究会	経済産業省において設置された研究会。我が国の産業が直面する、深刻度を増しているサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される。
し	事業継続計画	BCPを参照。
	重要インフラサービス	重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。
	重要インフラサービス障害	重要インフラの情報セキュリティ対策に係る第４次行動計画において新設した用語。システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
	重要インフラ所管省庁	重要インフラの情報セキュリティ対策に係る第３次行動計画及び同第４次行動計画における関係主体の一つ。金融庁、総務省、厚生労働省、経済産業省及び国土交通省。
	重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書	2018年４月４日サイバーセキュリティ戦略本部決定。情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的としているもの。
	重要インフラの情報セキュリティ対策に係る第４次行動計画	2017年４月18日サイバーセキュリティ戦略本部決定。昨今のサイバー攻撃による急速な脅威の高まりや、2020東京オリンピック・パラリンピック競技大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。「重要インフラ行動計画」、「第４次行動計画」と略称を使うことがある。

	重要インフラ分野	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、物流、化学、クレジット及び石油。重要インフラの情報セキュリティ対策に係る第４次行動計画において記載。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JIS Q 27000:2014）
	情報セキュリティ関係機関	重要インフラの情報セキュリティ対策に係る第３次行動計画及び同第４次行動計画における関係主体の一つ。警察庁サイバーフォースセンター、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人ICT-ISAC、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
	情報セキュリティ政策会議	2005年５月、IT総合戦略本部の下に設置された会議。内閣官房長官を議長とし、我が国の情報セキュリティに関する諸問題に係る対策等を決定する。サイバーセキュリティ戦略本部に業務が引き継がれ、2015年６月に廃止。
	情報セキュリティ普及啓発プログラム	今後推進すべき新たな普及啓発の進め方についてまとめたプログラム。2011年７月８日情報セキュリティ政策会議決定。改定版である新・情報セキュリティ普及啓発プログラムは2014年７月10日情報セキュリティ政策会議改定。
	情報通信ネットワーク安全・信頼性基準	1987年２月14日郵政省告示第73号。情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標としての基準を定めることにより、安全・信頼性対策の普及を促進し、もって情報通信ネットワークの健全な発展に寄与することを目的としているもの。
す	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的。
せ	制御系	センサーやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群をさす。
	セキュリティ・キャンプ協議会	次代を担う日本発で世界に通用する若年層のセキュリティ人材を発掘・育成するため、産業界、教育界を結集した講師による「セキュリティ・キャンプ」（22歳以下を対象）を実施し、それを全国的に普及、拡大していくことを目的とした協議会。なお、同協議会は2018年４月24日に「一般社団法人セキュリティ・キャンプ協議会」となったことが発表されている。
	セキュリティ・バイ・デザイン	システムの企画・設計段階から情報セキュリティの確保を盛り込むこと。
	セプター	CEPTOAR （Capability for Engineering of Protection, Technical Operation, Analysis and Response）を参照。
た	大規模サイバー攻撃事態	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。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。
つ	つながる世界の開発指針	IPAにおいて、2016年３月に策定、2017年６月に第２版へ改訂。様々なモノがつながって新たな価値を創出していく『つながる世界』ならではの機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項をとりまとめたもの。
て	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	技術や機器の検証・評価のための実証実験、又はそれを行う実験機器や条件整備された環境のこと。
	電気通信事業における個人情報保護に関するガイドライン	2017年４月18日総務省告示第152号。同年９月14日総務省告示第297号最終改正。電気通信事業の公共性及び高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信役務の利便性の向上を図るとともに、利用者の権利利益を保護することを目的とするもの。
	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。

と	統一基準群	国の行政機関、独立行政法人及び指定法人の情報セキュリティを確保するため、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関の情報セキュリティ対策のための統一規範」、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「政府機関の情報セキュリティ対策のための統一基準」（2016年８月31日サイバーセキュリティ戦略本部決定）及び「府省庁対策基準策定のためのガイドライン」（2016年８月31日内閣官房内閣サイバーセキュリティセンター決定）。
な	内閣サイバーセキュリティセンター	NISCを参照。
	ナショナルサイバートレーニングセンター	2017年４月、実践的なサイバートレーニングを企画・推進する組織としてNICTに設置されたもの。
	なりすまし	他の利用者のふりをすること。または、中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話。（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月、第４回：2016年７月、第５回：2017年７月）
は	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	秘密情報の保護ハンドブック～企業の価値向上に向けて～	経済産業省において、2016年２月に策定。秘密情報の漏えいを未然に防ぐため、企業が対策を行う際の参考となる対策例を紹介するもの。
	秘密情報の保護ハンドブックのてびき～情報管理も企業力～	経済産業省において、2016年12月に策定。「秘密情報の保護ハンドブック～企業の価値向上に向けて～」について、活用しやすいようにわかりやすくまとめたもの。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取、又は、組織等のシステムを破壊・妨害しようとする攻撃。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。
ふ	フィッシング	実在の金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為のこと。
	フィッシング対策協議会	フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、2005年４月28日に設立された協議会。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
へ	ベストプラクティス	優れていると考えられている事例やプロセス、ノウハウなど。

	ペネトレーションテスト	情報システムに対する侵入テストのこと。「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015年５月25日サイバーセキュリティ戦略本部決定）においては、「インターネットに接続されている情報システムについて、疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。」とされている。
ほ	ボットネット	マルウェアに感染したコンピュータ等により構成されたネットワークであり、攻撃者はネットワークを構成するコンピュータ等に対して一斉に指令を与えることができる。
	ポータルサイト	インターネットにアクセスする際の入口となるウェブサイト。
ま	マイナポータル	政府が運営するオンラインサービス。子育てに関する行政手続きがワンストップでできたり、行政機関からのお知らせを確認できたりするポータルサイトのこと。
	マルウェア	malicious software の短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。
み	未踏IT人材発掘・育成事業	2000年度から「未踏ソフトウェア創造事業」として開始し、2008年度により若い人材の発掘・育成に重点化すべく「未踏IT人材発掘・育成事業」として再編したもの。
り	リスクマネジメント	リスクを組織的に管理し、損失などの回避・低減等を図るプロセスのこと。
	リテラシー	本来、文字を読み書きする能力を意味するが、「情報リテラシー」のように、その分野における知識、教養、能力を意味することに使われている。
	量子暗号	量子力学の原理を用いた暗号技術。原理的に盗聴の有無を検知できる特性を持つ。

参考 2　担当府省庁一覧

項目	担当府省庁 （◎：主担当、○：関係府省庁）
1.　経済社会の活力の向上及び持続的発展	
1.1　新たな価値創出を支えるサイバーセキュリティの推進	
(1)　経営層の意識改革	◎：NISC、経済産業省 ○：金融庁
(2)　サイバーセキュリティに対する投資の推進	◎：総務省、経済産業省
(3)　先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化	◎：経済産業省 ○：総務省
1.2　多様なつながりから価値を生み出すサプライチェーンの実現	
(1)　サイバーセキュリティ対策指針の策定	◎：経済産業省
(2)　サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築	◎：内閣府 ○：総務省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(3)　中小企業の取組の促進	◎：NISC、総務省、経済産業省
1.3　安全な IoT システムの構築	
(1)　IoT システムにおけるサイバーセキュリティの体系の整備と国際標準化	◎：NISC、総務省、経済産業省
(2)　脆弱性対策に係る体制の整備	◎：NISC、警察庁、総務省、経済産業省
2.　国民が安全で安心して暮らせる社会の実現	
2.1　国民・社会を守るための取組	
(1)　安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、内閣府、宮内庁、警察庁、消費者庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：内閣官房副長官補（国土交通、海上保安担当） ※内閣府（◎）：政策統括官（科学技術・イノベーション担当）
(2)　サイバー犯罪への対策	◎：警察庁、総務省、法務省、経済産業省
2.2　官民一体となった重要インフラの防護	
(1)　行動計画に基づく主な取組	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、警察庁
(2)　地方公共団体のセキュリティ強化・充実	◎：NISC、内閣府、総務省 ○：内閣官房 ※内閣府：番号制度担当室、個人情報保護委員会
2.3　政府機関等におけるセキュリティ強化・充実	
(1)　情報システムのセキュリティ対策の高度化・可視化	◎：NISC、総務省、厚生労働省、経済産業省
(2)　クラウド化の推進等による効果的なセキュリティ対策	◎：NISC、内閣官房、総務省、経済産業省 ※内閣官房：情報通信技術（IT）総合戦略室
(3)　先端技術の活用による先取り対応への挑戦	◎：NISC
(4)　監査を通じたサイバーセキュリティの水準の向上	◎：NISC ○：内閣府、消費者庁、総務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産

	業省、国土交通省、環境省、防衛省
(5)　組織的な対応能力の充実	◎：NISC、総務省 ○：人事院
2.4　大学等における安全・安心な教育・研究環境の確保	
(1)　大学等の多様性を踏まえた対策の推進	◎：文部科学省 ○：NISC
(2)　大学等の連携協力による取組の推進	◎：文部科学省
2.5　2020 年東京大会とその後を見据えた取組	
(1)　2020 年東京大会に向けた態勢の整備	◎：NISC、警察庁
(2)　未来につながる成果の継承	◎：NISC、警察庁、総務省、法務省
2.6　従来の枠を超えた情報共有・連携体制の構築	◎：NISC、警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省
(1)　多様な主体の情報共有・連携の推進	◎：NISC
(2)　情報共有・連携の新たな段階へ	◎：NISC
2.7　大規模サイバー攻撃事態等への対処態勢の強化	◎：NISC、内閣官房、内閣府、警察庁、経済産業省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、内閣府：個人情報保護委員会
3.　国際社会の平和・安定及び我が国の安全保障への寄与	
3.1　自由、公正かつ安全なサイバー空間の堅持	◎：NISC ○：外務省
(1)　自由、公正かつ安全なサイバー空間の理念の発信	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省
(2)　サイバー空間における法の支配の推進	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省
3.2　我が国の防御力・抑止力・状況把握力の強化	
(1)　国家の強靱性の確保	◎：NISC、内閣官房、警察庁、法務省、文部科学省、防衛省 ○：内閣府、総務省、外務省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省 ※内閣官房：内閣情報調査室
(2)　サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省 ※内閣官房：国家安全保障局
(3)　サイバー空間の状況把握の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：NISC、総務省、外務省 ※内閣官房：国家安全保障局、内閣情報調査室
3.3　国際協力・連携	◎：NISC ○：その他の府省庁
(1)　知見の共有・政策調整	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省 ○：法務省
(2)　事故対応等に係る国際連携の強化	◎：NISC、経済産業省 ○：警察庁、外務省
(3)　能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省
4.　横断的施策	
4.1　人材育成・確保	◎：NISC ○：総務省、文部科学省、経済産業省
(1)　戦略マネジメント層の育成・定着	◎：NISC、文部科学省、経済産業省
(2)　実務者層・技術者層の育成	◎：警察庁、総務省、文部科学省、厚生労働省、経済産業省、防衛省 ○：NISC

(3)　人材育成基盤の整備	◎：総務省、文部科学省、経済産業省
(4)　各府省庁におけるセキュリティ人材の確保・育成の強化	◎：NISC、総務省 ○：その他の府省庁
(5)　国際連携の推進	◎：NISC、経済産業省
4.2　研究開発の推進	
(1)　実践的な研究開発の推進	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(2)　中長期的な技術・社会の進化を視野に入れた対応	◎：NISC ○：その他の府省庁
4.3　全員参加による協働	◎：NISC、総務省、文部科学省、経済産業省 ○：法務省
5.推進体制	◎：NISC、内閣官房 ○：総務省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）