資料３

サイバーセキュリティ 2015（案）

資料３－１　サイバーセキュリティ 2015（案）の概要

※資料３－２　サイバーセキュリティ 2015（案）

※は、パブリックコメントを行うものとしてサイバーセキュリティ戦略本部決定を行う案。

「サイバーセキュリティ2015(案)」の概要について

資料３－１

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

- IoTに係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】
- M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】
- エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】
- 経営ガイドラインの策定【経済産業省】
- 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】
- ISACを活用した情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 政府系ファンド等の活用検討【経済産業省】
- 著作権法におけるリバースエンジニアリングに関する適法性を明確化【文部科学省】
- 制御システムセキュリティ認証の拡大【経済産業省】

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

- マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】
- 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】
- 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】

■重要インフラを守るための取組

- オリンピック・パラリンピック東京大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】
- マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】

■政府機関を守るための取組

- 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】
- 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保

- 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】
- カウンターインテリジェンスに係る取組の推進【内閣官房】
- サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】
- 部外インフラ等、関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 二国間協議や多国間協議に参画し、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、我が国の意向を反映【内閣官房及び外務省】
- 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】
- 各国における能力構築を支援【内閣官房 他】

■世界各国との協力連携

- ASEAN諸国との連携を強化【内閣官房 他】
- 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、米国との情報共有を強化【総務省】
- 包括的な日米サイバー防衛の連携【防衛省】

横断的施策

■研究開発の推進

- 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】
- 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】

■人材の育成・確保

- 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人材の育成【文部科学省及び経済産業省】
- 初等中等教育に携わる教員等を対象とした研修、情報交換【文部科学省】
- 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】
- サイバー防御演習を通じた実践的セキュリティ人材の育成【総務省】

推進体制

- 伊勢志摩サミットにおけるサイバーセキュリティの確保やオリンピック・パラリンピック東京大会に向けた対策の検討【内閣官房】

資料３－２

サイバーセキュリティ２０１５

（案）

2015 年　　月　　日

サイバーセキュリティ戦略本部

目　次

はじめに

サイバー空間は、「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」であり、いまや欠くことのできない経済社会の活動基盤となっている。その一方で、国家の関与が疑われるような組織的かつ極めて高度なサイバー攻撃等による脅威の高まりが見られる状況にあり、サイバーセキュリティの確保は国民生活や社会経済活動、我が国の安全保障の観点から極めて重要な課題となっている。

こうした状況を背景に、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティ基本法（以下「基本法」という。）が昨年11月に成立し、政府は同法の規定に基づき、我が国のサイバーセキュリティ政策に関する新たな国家戦略となる「サイバーセキュリティ戦略」（以下「戦略」という。）を今後閣議決定する予定である。この戦略は、2020年オリンピック・パラリンピック東京大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後３年程度のサイバーセキュリティ政策の基本的な方向性を示すものであり、関係者の共通の理解と行動の基礎となるものである。

本書は戦略に基づく最初の年次計画であり、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2015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、戦略の基本原則にも示されているとおり、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. 安全なIoTシステムの創出

(1) 安全なIoTシステムを活用した新規事業の振興

(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。

(2) IoTシステムのセキュリティに係る体系及び体制の整備

(ア)内閣官房において、IoTシステムに係る大規模な事業のサイバーセキュリティ確保のための取組について、サイバーセキュリティ戦略本部の下で検討を進めるとともに、IT総合戦略本部等においても現在検討が進められているIoTシステムに係る大規模な事業について、関係省庁が適切に協働し、セキュリティ・バイ・デザインの考え方に基づいて必要な対策が整合的かつ遺漏なく実施されていくよう働きかけを行うとともに、その確認を適時確認していく。

(3) IoTシステムのセキュリティに係る制度整備

(ア)経済産業省において、IPAを通じて、IoTシステムに含まれる機器等に関して、攻撃事例や利用形態を基に整理を行い、総合的なガイドラインや基準の確立に向け、脅威分析とセキュリティ対策の明確化を図る。

(イ)総務省において、IoTシステムに関する横断的な取組の１つとして、ウェアラブル端末等のM2M機器の運用の実装上のセキュリティに係る横断的なガイドライン策定の検討を実施する。

(ウ)経済産業省において、エネルギー分野におけるIoTのセキュリティガイドラインとして、スマートメーターのセキュリティの評価技術・手順の実証を行う。

(エ)厚生労働省において、医薬品医療機器法上の医療機器のサイバーセキュリティについて検討を進める。

(オ)総務省において、自動車分野におけるIoTのセキュリティガイドラインとして、「700MHz帯安全運転支援システムのセキュリティガイドライン」を策定する。

(カ)経済産業省において、CSSCを通じ、IoTシステムの構成要素であるM2M機器等のセキュリティに係る認証制度であるEDSA認証（2014年４月開始）について、普及・啓発を行うとともに、制御システム全体のセキュリティ認証制度を確立する。

(キ)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。

(ク)経済産業省において、経済産業省告示により指定されたIPA（受付機関）とJPCERT/CC（調整

機関）により運用されている「脆弱性関連情報届出受付制度」により、IoTシステムを作動させるソフトウェアに係る脆弱性について、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」などを通じて、利用者に提供する。また、IPA（受付機関）とJPCERT/CC（調整機関）は、脆弱性が届出されたものの、連絡がつかない案件について、経済産業省告示に基づいた手続きの上、公表を行う。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。

(ケ)総務省において、脆弱性を有するブロードバンドルータ等のIoT製品について、ISP事業者等を通じ利用者に対策を促す仕組みの構築に向けた検討を実施する。

(4) IoTシステムのセキュリティに係る技術開発・実証

(ア)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品質、安全性、効率を向上、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。

(イ)総務省において、IoTシステムの構成要素の特徴を加味したセキュリティ技術の確立に向けた調査・実証を実施する。

(ウ)経済産業省において、CSSCにおける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を開発し、評価・認証制度やサイバー演習へと活用する。

(エ)総務省において、IoTシステムにおけるセキュリティ技術の確立に向け、IoT機器及びその運用基盤に対する脅威分析及びリスク評価を行う。

(オ)総務省及び経済産業省において、IoT機器へのバックドア対策のためのログ検知技術の開発に関する研究や、高信頼な暗号の実装を実現する技術やハードウェアトロージャン検知の技術等ハードウェアの真正性の向上に係る技術の開発に関する研究、IoTシステムに対応したセキュリティ評価認証制度の確立に向けた検討を行う。

(カ)経済産業省において、自動車のセキュリティ確立に向けて、自動車業界関係者等と制御システム等に関するセキュリティ上の課題と対策について情報交換を行い、解決に向けた方向性を得るとともに研究開発を推進する。

1.2. セキュリティマインドを持った企業経営の推進

(1) 経営層の意識改革

(ア)内閣官房及び金融庁において、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、米国の証券取引委員会（SEC）における取組等を参考にしつつ、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し、結論を得る。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し、結論を得る。

(イ)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、サイバーセキュリティ対策の在り方、CISOの設置を含めた組織体制の在り方、技術的対策、情報開示の在り方等を含めたサイバーセキュリティ経営ガイドラインを年内のできるだけ早

期に策定する。また、当該ガイドラインも含めた企業の取り組みについて、第三者認証等によりステークホルダー等から評価される仕組みを検討する。さらに、経済産業省において、実効性を高めるため、同ガイドラインの内容や利活用の在り方も含めた指針の法制度化を、中小企業向けも含めて検討する。

(ウ)経済産業省において、情報の保護が必要となる政府の補助事業や研究開発事業等の採択に際して、上記のサイバーセキュリティ経営ガイドラインや第三者認証取得など企業のサイバーセキュリティ対策への取り組みを、加点要素等として考慮する仕組みを検討する。

(2) 経営能力を高めるサイバーセキュリティ人材の育成

(ア)内閣官房及び経済産業省において、実務者層のリーダー層が「橋渡し人材層」として活躍できるよう、経営層の示す経営方針を踏まえたサイバーセキュリティに係るビジョンの策定能力や、こうしたビジョンを経営層及び実務者層に伝えていくコミュニケーション能力の向上を図るためのセミナー等を実施する。

(3) 組織能力の向上

(ア)内閣官房において、企業における製品・サービスの関係者を対象に、セキュリティ・バイ・デザインを共通の価値として認識させることを目指したセミナーの開催等の普及啓発活動を行う。

(イ)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。

(ウ)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、最新のサイバー攻撃の手口を踏まえたサイバーセキュリティ対策の在り方、組織体制の在り方、最新の攻撃に対する技術的対策、情報開示の在り方等を含めたサイバーセキュリティ経営ガイドラインを年内のできるだけ早期に策定し、企業に対して発信していく。また、当該ガイドラインも含めた企業の取り組みについて、第三者認証等によりステークホルダー等から客観的に評価される仕組みを検討する。

(エ)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発注者が把握できない多重の再委託などを防止し、情報システム開発・運用に係る取引の適正化を図るための制度整備を行う。

(オ)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。

(カ)総務省において、企業における標的型攻撃への対処能力の向上に向けた実践的な防御演習（CYDER）を実施する。

(キ)経済産業省において、企業への標的型攻撃への対処能力向上のため、CSSCにおける模擬システム等を用いた実践的なサイバー演習を行う。

(ク)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。

(ケ)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。

(コ)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が情報ハブとなり実施している「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。

(サ)総務省において、ISP事業者を中心に構成されている「Telecom-ISAC Japan（一般財団法人データ通信協会テレコム・アイザック推進会議)」を核として、サイバー攻撃に関する情報共有網の拡充を進める。

(シ)金融庁において、金融機関に対し、2014年11月から本格的に活動を開始した「金融ISAC」を含む情報共有機関等を通じた情報収集・共有体制の構築を促していく。

1.3. セキュリティに係るビジネス環境の整備

(1) サイバーセキュリティ関連産業の振興

(ア)経済産業省において、NEDOの支援事業や政府系ファンドによるベンチャー企業や国内外で大規模に活躍できる企業の育成など、サイバーセキュリティの成長産業化に取り組む。

(イ)総務省及び経済産業省において、クラウドセキュリティガイドライン、クラウドセキュリティ監査制度の普及促進を行う。

(ウ)総務省及び経済産業省において、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の関連税制の利用促進等、中小企業の情報セキュリティ対策の底上げを支援する施策を推進する。

(エ)文部科学省において、著作権法におけ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適法性の明確化に関する措置を速やかに講ずる。

(2) 公正なビジネス環境の整備

(ア)経済産業省において、関係省庁及び産業界の協力の下、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」を設置する。

(イ)経済産業省において、企業の重要情報である営業秘密の管理手法等の一層の高度化に資する

ため、人事・労務面、情報セキュリティなど多面的な対策について、最新の技術開発や内外の不正な営業秘密侵害事例を踏まえ、「営業秘密保護マニュアル（仮称）」として策定し、公表する。

(ウ)経済産業省において、IPAを通じて、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の普及促進を図る。

(エ)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。

(3) 我が国企業の国際展開のための環境整備

(ア)総務省及び経済産業省において、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。

(イ)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。

(ウ)経済産業省において、2014年に改訂した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を新たな国際標準（ISO/IEC27017）のベースとして組み入れるべく、国際標準化を推進する。

(エ)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。

(オ)経済産業省において、IPAによるCCRAなどの海外連携を通じ、セキュリティ評価に係る国際基準の作成に貢献するとともに、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。

(カ)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12ヶ国・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、マレーシア、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。

(キ)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、日本企業が安全に活動でき、また、日本の持つノウハウを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。

(ク)経済産業省において、JPCERT/CCを通じて、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。

(ケ)経済産業省において、CSSCが実施している制御システムセキュリティにかかる認証制度について、国際標準化の推進とそれをベースにした国際的な相互承認の対象制度の拡大を推進する。

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

(ア)内閣官房において、事業者のセキュリティ・バイ・デザインに対する取組を促すとともに、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行う。

(イ)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。

(ウ)経済産業省において、IPAを通じて流通後の修正が容易でないとされる組込みソフトウェア及びスマートフォン等のアプリケーションにおいて多用される言語に関し、IPAにおいて整備したコーディングスタンダードについて、更なる開発の高信頼化を図るための取組等を行う。

(エ)経済産業省において、IPAを通じて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」と体験的かつ実践的に学ぶツール「AppGoat」についてIPAを通じて普及啓発を図る。

(オ)経済産業省において、IPAを通じて、情報処理システム等におけるソフトウェアの不具合が社会に与える混乱や被害を防止する観点から、更なる開発・検証技術の高度化を図りつつ、ソフトウェアによって中核機能が実現される製品、システム及びサービスについて第三者がその安全性・信頼性等を利用者に対し十分に説明できるよう、利用者への品質説明力を強化する。

(カ)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「脆弱性関連情報届出受付制度」を着実に実施するとともに、関係者との連携を図りつつ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」の運用などにより、脆弱性関連情報をより確実に利用者に提供する。また、連絡不能案件について、経済産業省告示に基づいた手続きのうえ、公表を行う。

(キ)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。

(ク)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。

(ケ)総務省において、NICTを通じ、運用するサイバー攻撃観測網（NICTER）について、センサーの高度化等による観測機能の強化を図るとともに、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。

(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、マルウェアに感染したユーザーを検知し、マルウェアの除去を促す取組（感染駆除）及び閲覧することでマルウェアに感染する悪性サイトへアクセスする利用者に注意喚起を行う取組（感染防止）を引

き続き実施する。

(サ)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情報共有システム（TSUBAME）の運用との連動等の有効活用やその高度化を進める。

(シ)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。

(ス)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。

(セ)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について検討する。

(ソ)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、利用者及びアクセスポイント設置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、利用者及びアクセスポイント設置者に対する周知啓発を実施する。

(2) サイバー空間利用者の取組の促進

(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」に基づき、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に関する普及啓発活動を推進する。特に、「サイバーセキュリティ月間」を中心とし、シンポジウムやサイバーセキュリティカフェ等の活動を通じ普及啓発活動を進めるとともに、児童生徒やその保護者ならびに学校の教職員を対象とした啓発活動や、サイバー空間の脅威や対策について学ぶ機会の少ない者に対する取組も推進する。

(イ)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ほか、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。

(ウ)総務省において、「サイバーセキュリティ月間」に合わせて、全国でサイバーセキュリティ関連セミナーを実施するとともに、総務省「国民のための情報セキュリティサイト」を通じて最新のセキュリティトピックに関する普及啓発を実施する。

(エ)総務省、法務省及び経済産業省において、電子署名の利活用に関するセミナーの開催及びHPを活用した電子署名の利活用策に関する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。

(オ)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」の実施や「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、関係者と連携して周知啓発のための取組を行う。

(カ)文部科学省において、児童生徒への指導に役立つ教員用動画教材及び指導手引書や子供たちがインターネット上で遭遇する課題について保護者向けの普及啓発教材を作成・普及する。

(キ)文部科学省において、全国の学校へ配布する普及啓発資料の作成や、フォーラム（東京で１回)、ネットモラルキャラバン隊（全国７カ所）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。

(ク)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」を一般国民に提供する。

(ケ)経済産業省において、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。

(コ)内閣官房において、関係省庁と協力し、関係府省庁が既に設置している情報セキュリティに関する相談窓口について、国民・利用者の視点に立ち、連携を強化するなど、相談体制を充実させる。

(サ)内閣官房において、産学官民が協議会等の形で連携し、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」等を活用しつつ必要な取組について検討を進める。

(シ)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。

(ス)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。

(セ)総務省において、関係機関と協力のうえ、地方公共団体職員がICT-BCP策定の必要性と基本事項を理解・習得することを支援するため、ICT-BCP策定セミナーを実施する。また、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。

(ソ)総務省において、関係機関と協力のうえ、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。また、地方公共団体における緊急時の対応について、マニュアルを提供

する等支援する。

(タ)総務省において、関係機関と協力のうえ、公開サーバやネットワーク機器等における脆弱性診断、Web感染型マルウェアによる改ざん検知を地方公共団体に対して実施する。また、脆弱性対策の知識向上を目的に実技形式の講習会等を全国２カ所で開催する。

(チ)総務省において、実践的な防御演習（CYDER）を、ものづくりの源泉としてサプライチェーンの一端を担う中小企業にも積極展開し、標的型攻撃への対処能力の向上を図る。

(ツ)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（仮称)」を実施するとともに、中小企業団体等との連携により、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「iSupport」等のツール等の利用促進等を図る。

(テ)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。

(ト)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相談窓口」を通じ、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り組みを支援する。

(ナ)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。

(3) サイバー犯罪への対策

(ア)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。

(イ)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、各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、総合セキュリティ対策会議等において官民連携による取組を推進する。

(ウ)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。

(エ)警察庁において、サイバー空間におけるボランティア活動の促進を図るため、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。

(オ)警察庁において、スマートフォン利用者等を狙ったサイバー犯罪に関し、情報セキュリティ関連事業者等との連携強化による情報集約等に努め、取締りの強化を図る。また、取締りにより判明した実態等を踏まえ、一般利用者等の情報セキュリティ対策の向上に資する情報発信等を推進する。

(カ)警察庁において、警察大学校サイバーセキュリティ研究・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。

(キ)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。

(ク)警察庁において、多様化・複雑化するサイバー犯罪に適切に対処するため、高度情報技術解析センターを中心に不正プログラムの効率的な解析を推進するとともに、サイバー犯罪捜査に従事する警察職員に対する研修の実施、資機材の増強、関係機関との協力等を通じ、デジタルフォレンジックに係る体制を強化する。

(ケ)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、捜査能力の充実を図る。

(コ)検察当局において、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）が施行されたことを踏まえ、その適正な運用を実施する。

(サ)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」の解説の改正を踏まえ、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. 重要インフラを守るための取組

(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３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。また、本年度内を目途に、更なるセキュリティ強化等の具体的内容について取りまとめる。

(イ)内閣官房において、各重要インフラ分野における安全基準等について、強制基準やガイドライン等の体系を明らかにする調査を実施する。その調査結果を踏まえ、安全基準等の体系を明示した調査項目を加えた安全基準等の改善状況調査を実施し、課題の抽出を行う。

(ウ)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、申告受付の夜間・休日の全国一元化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研究を実施する。

(エ)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。

(オ)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、重要インフラにおける標的型攻撃への対処能力を向上させ、重要インフラの持続的なサービス提供に向けた実践的な防御演習（CYDER）を実施する。
- 経済産業省において、CSSCを通じて、重要インフラ等企業における標的型攻撃に対する対応能力を向上させるため、模擬システムを活用した実践的なサイバー演習を実施する。

(1) 重要インフラ防護の範囲等の不断の見直し

(ア)内閣官房において、重要インフラ所管省庁等との連携の下、2020年のオリンピック・パラリンピック東京大会をテストケースとして、情報システムの障害が当該大会の開催に重大な影響を与えるサービス、それを提供する事業者及びその分野の候補を選定すると共に、所管省庁や事業者が行うリスク評価を支援するための手順を整備する。前記取組により得られた知見も活用し、新たな重要インフラ分野や事業者の候補を選定する。

(イ)内閣官房において、重要インフラ所管省庁の協力の下、第３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、取組を拡大する対象として、重要インフラ事業者等が提供するサービスに間接的に関わる外部委託先や主要関係先の洗い出しを行う。

(ウ)内閣官房において、重要インフラ分野以外の民間企業をサイバー攻撃から保護するために、既存の重要インフラ分野いかんに関わらず情報共有等の取組の対象とすべき企業の範囲について検討を行う。

(2) 効果的かつ迅速な情報共有の実現

(ア)内閣官房において、重要インフラ所管省庁の協力の下、サイバー攻撃に対するより効果的な情報を迅速に共有するための在り方を検討すると共に、小規模な障害情報や予兆情報（ヒヤリハット等）の情報共有について政府機関内での連携強化を図る。

(イ)経済産業省において、官民における最新の脅威情報やインシデント情報等の共有のため、IPAが情報ハブとなり実施している「サイバー情報共有イニシアティブ」（J-CSIP）について参加組織の拡大、共有情報の充実を行う。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、障害事例や提供情報の分析結果等を重要インフラ事業者等へ提供する。

(ウ)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。また、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。

(エ)内閣官房において、情報セキュリティ関係機関と協力関係を構築・強化していくと共に、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。

(オ)総務省において、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、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整備・構築に向けた検討を行う。

(カ)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、関係省庁との情報共有等を通じて、サイバー攻撃事案の攻撃者や手口の実態解明に係る情報収集・分析を継続的に実施する。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とともに、重要インフラ事業者等の意向を尊重し、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を行う。
・ 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。

(3) 各分野の個別事情への支援

(ア)内閣官房において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対して情報の提供など、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)内閣官房及び総務省において、総合行政ネットワーク（LGWAN）について集中的にセキュリティ監視を行う機能を設けるなどして、GSOCとの情報連携を通じた、国・地方全体を俯瞰した監視・検知体制を整備するとともに、地方公共団体のセキュリティ対策に関する支援の強化を図ること等により、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。また、情報提供ネットワークシステム等のマイナンバー関係システムについて、インターネットから独立する等の高いセキュリティ対策が講じられたものとなるよう、管理・監督・支援等を行う。加えて、特定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立ち上げるとともに、監視・監督方針を速やかに策定するなど、本年度中を目途に、監視・監督体制を整備する。

(ウ)内閣官房において、マイナンバー制度の下で認証連携を行うに当たって、利便性の向上とセキュリティの確保がバランスの取れたものとなるよう、政府内及び官民での認証連携について、多要素認証等の認証方式や連携条件についての検討を行い、本年中を目途に取組方針を策定する。

(エ)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、経済産業省において、経済産業省告示に基づき、IPAとJPCERT/CCにより運用され、制御システムの脆弱性情報の届出も受け付ける「脆

弱性関連情報届出受付制度」を運用する。

(オ)経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、CSSCを通じて、セキュリティ対策に関する知見を収集し、それに基づいたセミナー及びより実践的な演習を実施する。

(カ)経済産業省において、CSSCが実施する制御機器のセキュリティ評価・認証の利用促進を図るとともに、制御システム全体のセキュリティに関する評価・認証制度の構築を行う。また、制御システムのセキュリティマネジメントシステム適合性評価スキームの普及について、JIPDEC等関係機関に対して支援を行う。さらに、CSSCの制御システムセキュリティテストベッド施設を利用した研究開発成果の展開を図り、その成果を用いて制御システムセキュリティに係る国際標準化の推進を図るとともに、それに基づいた国際的な相互承認制度の拡大を推進する。

2.3. 政府機関を守るための取組

(ア)内閣官房において、新たに直面した脅威・課題への対応について、政府統一基準を始めとした規程に適時反映するため、政府統一基準等の次期改定に向けた検討を順次進める。

(1) 攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進

(ア)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、諸外国におけるSOC事例の調査を行い、その結果を踏まえ、GSOCが有するべき機能、政府機関等の連携体制等について、検討を行う。

(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、GSOC、CYMAT、各府省庁CSIRT等の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を形成する。

(ウ)内閣官房において、政府機関における情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組（SBD）を推進するため、サプライチェーン・リスクへの対応を含むSBDの観点から情報システムの調達仕様書に確実に記載すべき事項について、各府省庁における事例を調査し、各府省庁と共有する。また、情勢変化に応じた運用中の情報システムにおける対策の迅速・柔軟な見直しの在り方について検討を行う。さらに、それらについて、政府機関全体として取り組むべき事項が把握された際には、政府統一基準を始めとした規程への反映に向けた検討を行う。

(エ)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。

(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、政府調達を推進するため、調達関係者に対する勉強会やヒアリングを実施するとともに必要に応じて見直

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、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、ペネトレーションテストを実施することにより、攻撃者が用いる手法で実際に侵入できるかどうかの観点から防御策の状況を検証し、改善のための必要な助言等を行う。

(ク)内閣官房において、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を調査し、各府省庁と共有するとともに、調査結果に応じて、政府統一基準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)総務省において、システムのログに基づいて標的型攻撃を検知し、被害を未然に防止等するための防御モデルの検討を行う。

(コ)内閣官房において、2020年オリンピック・パラリンピック東京大会も念頭に置きつつ、インシデント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、設置対象の法人等の段階的追加を含む監視対象の拡大を行うための具体的方策の検討を行う。

(サ)内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能の強化を図るため、情報システムにおけるログの取得や活用の在り方について、サイバー攻撃を受けた際の影響範囲の特定、原因究明等の観点から検討を行う。

(シ)内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能及び要員間の連携の強化を図るため、各府省庁のCSIRT体制やインシデント対処に係る現状の課題等について、CISOを始めとした幹部による指揮の下での組織的対処の観点も含めて調査し、各府省庁と共有するとともに、調査結果に応じて、要員のキャリアパスの構築等にも配慮しつつ、CSIRTの体制の拡充や実効性の向上に取り組むとともに、政府統一基準を始めとした規程への反映について検討を行う。また、調査結果については、各府省庁と共有を図る。

(ス)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、各府省庁における対処要員を対象として、サイバー攻撃発生時におけるCISOを始めとした幹部による指揮の下での迅速かつ適切なインシデントへの組織的対処及び確実な連携（独立行政法人等を所管する部局との連携等を含む。）の実現を目指し、インシデント・ハンドリングを中心として近年のサイバー攻撃動向を踏まえた訓練を平素から実施する。
- 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）要員等に対する訓練等を技術的事項の習得に重点を置いて実施する。
- 総務省において、政府機関における標的型攻撃への対処能力の向上に向け、新たなシナリオによる実践的な防御演習（CYDER）を実施する。

(セ)内閣官房において、政府職員のインシデント・ハンドリング能力等を向上させていくため、

2014年度に初めて開催したサイバー攻撃対処能力を競うNATIONAL 318(CYBER) EKIDENを、さらに発展させていくべく取り組む。

(ソ)内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能の強化を図るため、各府省庁のCSIRT等が、サイバー攻撃発生時に外部の専門家等による必要な支援をより迅速に得られるようにするための体制・制度の構築に取り組むとともに、政府統一基準を始めとした規程への反映に向けた検討を行う。

(タ)内閣官房において、GSOCシステム等による監視効率の向上等によりリスクを低減させるため、業務効率にも留意しつつ、各府省庁の情報システムの集約化に合わせたインターネット接続口の早急な集約化を行うことによる攻撃リスクの低減等を含む政府機関等の対策方針を早急に取りまとめるとともに、政府統一基準を始めとした規程への反映に向けた検討を行う。

(チ)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適切に始動させるため、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。

(ツ)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の加速を図るとともに、個人情報や機微な情報を始めとした機密性・完全性の高い情報に焦点を当てた政府機関における情報管理の更なる強化に向けて、取り扱う情報の性質や量に応じた情報システムの分離、機密性・完全性の高い情報を管理するデータベースに対する不正なアクセス等による情報漏えいや改ざん等への対策について政府統一基準を始めとした規程への反映に向けた検討を行う。

(テ)内閣官房において、リスク評価に基づく重点的な対策実施を推進するとともに、リスクや影響度に応じたインシデント対処や情報システムの対策強化に関する優先度の評価方法について、その在り方に関する検討を行う。

(2) しなやかな組織的対応能力の強化

(ア)内閣官房において、政府機関における政府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、点検を目的とした従来の施策等の統合も視野に入れた監査制度を設計するとともに、当該制度の有効性の検証を目的として、試行的な監査を実施する。試行的な監査については、各府省庁が実施しているセキュリティ監査の評価を監査テーマとして実施するとともに、次年度以降の本格的な監査制度の運用に資することを考慮し、各府省庁のサイバーセキュリティ対策及びその維持改善体制の整備及び運用状況に係る現状を把握し、改善に資する対応策について助言等を行う。また、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等を内閣官房が実施する監査及び原因究明調査の対象とすることを検討した上で、当該法人の業務等の性質やセキュリティ対策の緊急性等に応じて監査等を実施する。さらに、当該法人を所管する府省庁と協力し、当該法人に対する監査等の在り方について検討を行う。

(イ)内閣官房において、リスク評価に基づく組織的な情報システムの対策・管理を推進するため、情報システムにおけるリスク対処方針、対策水準、事態の緊急度に応じた意思決定プロセス等を情報システムのユーザー側と管理側との双方の合意に基づき、CIO補佐官や最高情報セキュリティアドバイザー等の外部から起用する人材の積極的な活用を図りつつ、組織的

に設定する制度について、その在り方に関する検討を行う。

(ウ)内閣官房において、政府機関における共通的な課題や未知の脅威等の顕在化に備えた対応に関するプラクティスの共有や意見交換を促進するためのコミュニティを形成する。

(エ)内閣官房において、各府省庁におけるけん引役となるセキュリティ人材の育成に資するため、各府省庁のセキュリティ担当者に加え、幹部職員や独立行政法人を所管する部局の担当者を対象に、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平素から開催する。また、各府省庁におけるサイバーセキュリティに関する職員教育を推進するため、教育資料のひな形の提供等による支援を行う。

(オ)内閣官房において、各府省庁による新規採用時のサイバーセキュリティに関する職員教育を支援するため、資料のひな形の提供等を行うとともに、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。

(3) 技術の進歩や業務遂行形態の変化への対応

(ア)内閣官房において、新たなIT製品・サービスの普及等に伴う政府統一的な対策の必要性を検討するため、各府省庁におけるクラウドサービス等の利用や対策の状況について調査するとともに、各府省庁と共有する。

(イ)内閣官房において、ITを活用した政府機関全体としての行政事務について、関係機関と連携し、サイバーセキュリティの確保が前提となった遂行形態の実現を図る。

(4) 監視対象の拡大等による総合的な対策強化

(ア)内閣官房において、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における政府機関の取組を踏まえた取組を総合的に強化するため、当該法人を所管する府省庁と協力し、当該法人における対策の実施状況を確認し、当該法人の対策強化を図る。また、当該法人において統一的に取り組むべき事項が把握された際には、当該法人の性質等を踏まえつつ、政府統一基準を始めとした規程への反映に向けた検討を行う。

3. 国際社会の平和・安定及び我が国の安全保障

3.1. 我が国の安全の確保

(ア)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、国内外におけるサイバー攻撃関連情報を収集・分析する体制の確立及び強化を実施するとともに、必要な機材の整備を行う。

(イ)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、関係府省庁等と連携した初動対処訓練を実施する。

(1) 対処機関の能力強化

(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)警察庁において、サイバー攻撃対策に係る体制等を強化するため、サイバー空間に関する観測機能の強化を図るとともに、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、サイバーテロ対策の強化のため、大規模産業型制御システムに対するサイバー攻撃対策に係る訓練を実施する。

(エ)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、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、防衛省情報通信基盤（DII）のクローズ系及びネットワーク監視器材へ最新技術を適用していく。

(オ)防衛省において、サイバー攻撃時においても、被害の拡大防止等対処能力を向上し継続的な部隊運用を確保するため、指揮系システムに係るサイバー演習環境の構築技術に関する研究の実施及び当該成果を踏まえて演習環境の構築を行う。また、将来の技術動向等を踏まえたサイバー攻撃対処能力の向上を目的として、相手方のサイバー空間の利用を妨げる能力に関する調査研究を行い、攻撃・防御機能及び統裁・評価機能等を備えた演習環境を整備する。

(カ)防衛省において、サイバー攻撃生起時における重要通信の優先的な経路確保を可能とするための最新技術の取得に向けた調査研究を実施する。

(キ)防衛省において、実践的な教育を実施し、巧妙化するサイバー攻撃に適切に対応していくため、体験学習型の手法を用いたeラーニングコンテンツに関する調査研究を実施するとともに、国内外の大学院等への留学等も引き続き行い、人材育成への取り組みを実施する。

(2) 我が国の先端技術の活用・防護

(ア)防衛省において、更なるサイバーセキュリティの確保を目的として、防衛省において調達す

る情報システムに使用される、部品等のトレーサビリティ（製造元の追跡）に関する調査研究を行う。

(イ)経済産業省において、我が国の先端技術の活用・防護を図るため、CSSCを通じて、システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を行う。

(3) 政府機関・社会システムの防護

(ア)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・実効的連携要領の確立等に向けた取組を実施する。また、任務保証の観点から、任務遂行上依存する部外インフラへのサイバー攻撃の影響に関する知見を向上し、関係主体との連携を深化させていく。

3.2. 国際社会の平和・安定

(ア)総務省において、近年、被害が拡大しているサイバー攻撃（DDoS攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外のISP、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するセンサーを設置し、諸外国と連携してサイバー攻撃の予兆を検知し迅速に対応することを可能とする技術について、その研究開発及び実証実験を実施する。本件技術開発にあたり、欧米、ASEAN諸国等との連携を進める。

(イ)経済産業省において、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情報共有システム（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。

(1) サイバー空間における国際的な法の支配の確立

(ア)内閣官房、警察庁、総務省、外務省、経済産業省、防衛省において、各二国間協議や国連サイバーGGE、APEC、OECD会合等の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、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。

(イ)外務省において、我が国が2012年７月にサイバー犯罪条約を締結し、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。

(ウ)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。

(エ)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/G8、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、外国法執行機関との連携を強化するため、職員を派遣する。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。

(2) 国際的な信頼醸成措置

(ア)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、国連の場を活用したルール作りに携わるとともに、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。これらの取組に当たっては、内閣サイバーセキュリティセンターをサイバーセキュリティに関する我が国の国際的な窓口（コンタクトポイント）とし、外務省及び関係府省庁と共同して対外的な情報発信を強化すると共に、把握したサイバーセキュリティに関する情報を国内の関係機関と共有する。

(イ)内閣官房及び関係府省庁において、各二国間協議やIWWN等のサイバー空間に関する多国間の国際会議等に参画し、それぞれの取り組みにおいてインシデント対応演習や机上演習等を通じて、各国との情報共有や国際連携、信頼醸成を推進し、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。

(ウ)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) サイバー空間を悪用した国際テロ組織の活動への対策

(ア)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。

(イ)警察庁及び法務省において、国際テロ組織等による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、人的情報収集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。

(4) サイバー分野における能力構築（キャパシティビルディング）への協力

(ア)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)内閣官房、警察庁、総務省、外務省、経済産業省、防衛省、その他関係府省庁において、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、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情報セキュリティ政策会議を通じた人材育成の取り組みやASEAN加盟国と連携したサイバーセキュリティに関する国際キャンペーンの取り組みを通じて、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）の開催等を通じ、アジア大洋州地域を始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、APEC電気通信・情報産業大臣会合を通じて、情報通信分野に関してAPEC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意識啓発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）における取り組みやITU-D等の取り組みを通じて、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２回日・ASEANサイバー犯罪対策対話やUNODCプロジェクトの枠組みを通じて、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、日本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。

(5) 国際的な人材育成

(ア)内閣官房及び関係府省庁において、各国機関との連携、国際会議への参加や留学の支援、我が国での国際会議の開催、現在国内で開催されている競技イベントを国際レベルで行うこと等を通じ、わが国の情報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。

3.3. 世界各国との協力・連携

(ア)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・運用面の協力に関する企画・立案機能を強化する。

(イ)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。

(ウ)内閣官房及び関係府省庁において、「サイバーセキュリティ国際キャンペーン」を実施し、サイバーセキュリティに関する国際的なイベントの開催や各国と連携した意識啓発活動を行うことで、幅広い範囲での国際協力体制を確立し、サイバー空間の安全を確保していく。

(エ)内閣官房、総務省、外務省、経済産業省及び関係府省庁において、これまで二国間対話等を実施してきた各国との枠組を継続するとともに、合意された連携を推進する。また、更なる連携の対象を検討し、必要があれば新たな二国間対話等の立ち上げを図り、国際協力体制を確立する。

(オ)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、攻撃主体・方法等に関する情報収集・分析を継続的に実施する。

(カ)経済産業省において、攻撃者が悪用する、グローバルに広がっている脅威や攻撃基盤等の問題に、各国のCSIRTが連携して対応・対策を実施するために必要となる、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。

(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より、米NIST等の各国の情報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)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等を行う。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。

(ケ)内閣官房において、外国関係機関との情報交換等を緊密に行い、主要国のサイバー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。

(1) アジア大洋州

(ア)防衛省及び関係府省庁において、東南アジア各国防衛当局との間のITフォーラム等の取組を通じ、サイバー分野での国際連携や能力構築への協力、情報の収集や発信を推進していく。

(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)内閣官房、総務省、外務省及び経済産業省において、日ASEAN情報セキュリティ政策会議の枠組みを通じ、ASEAN加盟国とのサイバー分野における連携を強化する。また、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。

(2) 北米

(ア)総務省において、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、サイバー攻撃に関するデータを共有及び研究開発の分野での協力関係の加速化という考えに基づき、データの共有などの米国との情報共有を強化する。

(イ)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、技術分野での協力において、包括的な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。

(ウ)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。

(3) 欧州

(ア)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 CCD COEにおける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。

(イ)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、JTEMSと定期的に協議を行う。

4. 横断的施策

4.1. 研究開発の推進

(ア)内閣官房において、各省庁と協力し、「情報セキュリティ研究開発戦略（改定版）」に基づき、情報セキュリティの研究開発を推進する。

(イ)総務省において、NICTを通じ、情報通信ネットワークの安全性を保証する上で、ルータ等のネットワーク機器に実装されている通信プロトコル等が安全性の高いものであるかを検証するための評価手法の確立に向けた研究開発を実施する。

(ウ)総務省において、NICTを通じ、ネットワークの各構成要素（ノード）における最適な情報セキュリティ設定を自動的に導出することを目指し、利用者環境のプライバシーを保護しつつネットワーク全体におけるリスク評価・検証技術の研究開発を実施する。

(エ)総務省において、NICTを通じ、2020年頃の実現を視野に、ユーザーからの要求に応じた最適な品質やセキュリティ・耐災害性等に優れた新世代ネットワークの基盤技術の研究開発を推進する。

(1) サイバー攻撃の検知・防御能力の向上

(ア)総務省において、NICTを通じ、標的型攻撃の対策技術として、マルウェアに感染したコンピュータからの情報流出に対処する技術の研究開発を行う。

(イ)総務省において、NICTを通じ、世界最先端のサイバー攻撃観測・分析・対策・予防技術、セキュアネットワークの設計・評価と最適構成技術、次世代暗号基盤技術等、ネットワークセキュリティ技術の研究開発を実施する。

(ウ)総務省において、利用者の行動特性等を利用した、標的型攻撃等の新たなサイバー攻撃への対策技術に関する研究開発を実施する。

(エ)経済産業省において、CSSCを通じて、システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を行う。

(オ)総務省において、NICTを通じ、サイバーセキュリティの研究開発を促進するため、攻撃トラフィック、マルウェア検体等のデータセットについて、大学等の外部の研究機関の安全な利用を可能にする研究基盤（NONSTOP）を運用する。

(カ)文部科学省において、NIIを通じ、サイバー攻撃耐性を向上させるため、大学等の関係機関において、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。

(キ)総務省及び経済産業省において、IoT機器へのバックドア対策のためのログ検知技術の開発に関する研究や、高信頼な暗号の実装を実現する技術やハードウェアトロージャン検知の技術等ハードウェアの真正性の向上に係る技術の開発に関する研究、IoTシステムに対応したセキュリティ評価認証制度の確立に向けた検討を行う。

(2) サイバーセキュリティと他分野の融合領域の研究

(ア)内閣官房において、各府省庁と連携し、法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進する。

(イ)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ー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。

(ウ)文部科学省において、ビッグデータやAI（人工知能）といった社会・技術の変化を先取りした調査・研究・開発についての検討を行っていく。

(3) サイバーセキュリティのコア技術の保持

(ア)総務省において、NICTを通じ、情報の円滑な利用を妨げず、必要な情報秘匿及び認証を両立するための研究開発を行う。

(イ)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。

(ウ)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、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、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討を実施するため、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。

(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品質、安全性、効率を向上、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)文部科学省において、科学技術基盤としてイノベーションを支える情報基盤に係る耐災害性強化（分散システム導入や自己修復機能の付加等）等、課題達成に貢献する機能の強化等をより一層推進するため、研究開発を実施する。

(4) 国際連携による研究開発の強化

(ア)総務省において、情報セキュリティ分野の国際標準化活動である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、国際規格への反映が行われるよう積極的に参画する。

(イ)総務省において、近年、被害が拡大しているサイバー攻撃（DDoS攻撃等、マルウェアの感染活動）に対処し、我が国におけるサイバー攻撃のリスクを軽減するため、国内外のISP、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するセンサーを設置し、諸外国と連携してサイバー攻撃の予兆を検知し迅速に対応することを可能とする技術について、その研究開発及び実証実験を実施する。

(5) 関係機関との連携

(ア)内閣府において、2015年６月18日の総合科学技術・イノベーション会議で追加が決定された、戦略的イノベーション創造プログラム（SIP）新規課題候補「重要インフラ等におけるサイバーセキュリティの確保」に対し、研究開発に向けた取組を推進する。

4.2. 人材の育成・確保

(ア)内閣官房において、関係府省庁と連携しつつ、「新・情報セキュリティ人材育成プログラム」に基づき関係施策を推進していく。

(イ)内閣官房において、人材育成に係る施策を総合的に推進するため、「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。

(ウ)経済産業省において、中長期スパンでの情報セキュリティを含めたIT人材育成の在り方について、引き続き、産業構造審議会商務流通情報分科会情報経済小委員会IT人材WGにおいて検討を進める。

(1) 高等教育段階や職業能力開発における社会ニーズに合った人材の育成

(ア)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演習を推進する体制の構築やPBL（課題解決型学習）の実施を支援する。

(イ)内閣官房において、関係府省庁と連携しつつ、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、実践的なサイバー演習環境の整備に向けた検討を行う。

(ウ)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。

(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。

(オ)内閣官房において、シンポジウムやセミナー等の啓発の場や情報共有の場を活用し、大学におけるサイバーセキュリティに関する教育の実施に資するような情報セキュリティに関する最新情報を提供する。

(カ)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。

(キ)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。

(ク)内閣官房において、行政機関等が入手したサイバーセキュリティに係る事案情報、不正プログラム情報や、行政機関自らが感知した事案情報等について、情報提供者の秘密保持等に配慮し、関係者の同意を得た上で、学習教材として教育・訓練等に活用される方法の検討を進

める。

(2) 初等中等教育段階における教育の充実

(ア)文部科学省において、学習指導要領を踏まえながら、児童生徒の発達段階に応じた情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進する。特に、論理的思考力の育成等に関しては、教員の指導の参考となるよう、発達段階に応じたプログラミングの指導手引書を作成する。また、情報モラルについては、教員の指導に役立つ動画教材及び指導手引書を作成・普及し、情報セキュリティを含む情報モラルに関する教育の充実を図る。

(イ)文部科学省において、初等中等教育に携わる全ての教員並びに教育委員会及び学校の全ての管理職等の情報セキュリティに関する基本的な知識を含む情報通信技術に関する指導力の向上を目指した取組が地方公共団体等において進められるよう、各地域で中核的な役割を担う指導主事、リーダー的教員等を対象とした研修や指導方法等に関する情報交換の機会の提供等を行う。

(ウ)内閣官房において、教育機関で育成する人材のレベルの明確化と併せて、そうした人材を育成する教員にとって必要となるスキル育成の場や教員向けの教材等について、民間の能力の活用や、一線を退いた技術者等が活躍できる環境整備も含め、産学官が相互に連携しながら検討を進める。

(3) 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

(ア)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・キャンプ実施協議会」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。

(イ)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法人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用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 CTF 2015」）について経済産業省において普及・広報の支援を行う。

(ウ)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。

(4) 人材が将来にわたって活躍し続けるための環境整備

(ア)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。

(イ)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（仮称）」の創設を検討する。

(ウ)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人材育成のため、ITサービス産業において求められる次世代の高度IT人材像を発信するとともに、学生や若手技術者が将来のキャリアパスをイメージできるように、新たなITサービスビジネスの創造事例をとりまとめ、広報・普及する。

(エ)経済産業省において、情報処理技術者試験にサイバーセキュリティに従事する者の実践的な能力を適時適切に評価するための更新制度を導入するため必要な措置をとる。加えて、行政機関等における人材登用でこれらの能力評価制度を積極的に活用する方策を検討する。

(5) 組織力を高めるための人材育成

(ア)防衛省において、高度化するサイバー攻撃等への適切な対処態勢を維持するため、人材育成の取組として、国内外の大学院等への留学等を推進する。

(イ)総務省において、官公庁や企業等組織における実践的サイバー防御演習（CYDER）の基盤の強化及び拡充を通じた実践的なサイバーセキュリティ人材の育成について検討を行う。

(ウ)防衛省において、指揮系システムについて、サイバー攻撃時においても部隊運用を継続するとともに、被害の拡大を防止するなどの事後対処能力の練度向上を目的としたサイバー演習環境の構築技術に関する研究を実施する。また、その研究成果を受け、自衛隊のサイバー攻撃対処部隊の事後対処能力の練度を向上させるため、一般的な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演習環境を整備する。

(エ)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・実効的連携要領の確立等に向けた共同訓練を実施する。

5. 推進体制

(ア)内閣官房において、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を進化させるため体制を整備するとともに情報共有システムの構築を行う。中期的には、オリンピック・パラリンピック東京大会を見据え、NISC内に専従のCSIRT組織を整備する。また、サイバーセキュリティに関し、司令塔機能を果たすため、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、オリンピック・パラリンピック東京大会を始めとする国際的なビッグイベントにおけるサイバーセキュリティを確実に確保するため、その運営に大きな影響を及ぼし得る重要システム・サービスを洗い出し、それらに対するリスク評価を実施する（2016年度以降本格実施）ために必要な評価手順等の整理を関連組織と連携して推進する。また、これら重要システム・サービスに対するサイバー攻撃への対応に係る関係主体との情報共有の中核的役割を果たすオリンピック・パラリンピックCSIRTの構築に向け、調査研究や関係主体との連携を通じて検討を行う。

(ウ)内閣官房において、2016年に開催される伊勢志摩サミット及び関連大臣会議におけるサイバーセキュリティの確保のため、一時的に会議場に設置される情報システムを含む政府機関情報システムにおける対策の徹底を図る。また、サミット等各会議の円滑な開催に不可欠な重要サービスを提供する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ため、重要インフラ所管省庁をはじめとする関係省庁と連携し、必要な対策を推進する。各会議開催期間における実践的な対処体制として、サイバーセキュリティ関係機関を含む関係主体間の迅速かつ的確な情報共有を可能とする体制を確立し、実践的な事案対処訓練を実施する。

(エ)内閣官房において、IPAとの連携をはじめ、高度セキュリティ人材の民間登用等によりNISCの対処能力の一層の強化を図り、インシデント発生時に適切にNISCへ情報が集約されるよう関係省庁（幹部クラスを含む）との迅速な情報共有体制を構築する。

(オ)内閣官房において、検知、判断、対処、報告といった一連の初動対処を見直し、幹部も含めた組織的対応体制の構築や政府全体での実践的訓練などを通じ、危機管理対応の一層の強化を図る。

参考　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。
	APEC	Asia-Pacific Economic Cooperationの略（エイペック）。アジア太平洋地域の21の国と地域が参加する枠組み。
	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。
	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、業務（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	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。
	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。
	CSSC	Control System Security Centerの略。技術研究組合制御システムセキュリティセンター。重要インフラの制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証等を担う。2012年３月設立。
	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。
	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	DDoS攻撃	Distributed Denial of Serviceの略。分散型サービス不能攻撃。大量のコンピュータが一斉に特定のサーバにデータを送出し、通信路やサーバの処理能力をあふれさせて機能を停止させてしまうサイバー攻撃。大規模な攻撃では、遠隔操作される等により数万台以上のコンピュータが攻撃に用いられているケースもある。
	DII	Defense Information Infrastructureの略。防衛省の基盤的共通通信ネットワーク。
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、2015年７月現在、世界70ヶ国の官・民・大学等321の組織が参加している。
G	G8	Group of Eightの略。主要８か国首脳会議。
	GSOC	Government Security Operation Coordination teamの略（ジーソック）。政府横断的な情報収集、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。
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。
	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。
	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。
	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-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。
	IT総合戦略本部	高度情報通信ネットワーク社会推進戦略本部のこと。ITの活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に適確に対応することの緊要性にかんがみ、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進するために、2001年１月、内閣に設置された。
	IWWN	International Watch and Warning Networkの略。2004年に、米国・ドイツの主導により創設された会合で、サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組の促進を目的としている。先進15ヶ国の政府機関が参加している。
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。
	JIPDEC	Japan Institute for Promotion of Digital Economy and Communityの略。一般財団法人日本情報経済社会推進協会。電子情報を高度かつ安全安心に利活用するための基盤整備や諸課題の解決を通じて情報経済社会の推進を図り、もって我が国の国民生活の向上及び経済社会の発展に寄与することを目的とする。
	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。我が国において各国関係機関と連携して、サイバー攻撃情報やシステムの脆弱性関連情報等を収集・分析し、関係機関に情報提供するとともに、サイバー攻撃発生時には、関係者間の連絡調整や、攻撃の脅威分析、対策の検討に関する支援活動等を実施している機関。1996年10月に「コンピュータ緊急対応センター」として発足。
	JTEMS	Joint Interpretation Library（JIL） Terminal Evaluation Methodology Subgroupの略。カード端末セキュリティに関する検討部会。
	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	JVN iPedia 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	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。

	NONSTOP	NICTER Open Network SecurityTest-Out Platformの略。NICTER（NICTが開発するインターネットで発生する様々なセキュリティ上の脅威を迅速に把握し、有効な対策を導出するための複合的なシステム。）が保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤。
O	OECD	Organization for Economic Co-operation and Developmentの略。経済協力開発機構。
P	PBL	Project Based Learningの略。課題解決型学習。
	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	SBD	Security By Designの略。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。
	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。
	SEC	Securities and Exchange Commissionの略。米国証券取引委員会。
	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。
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。
	暗号モジュール試験及び認証制度	電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者による試験及び認証を組織的に実施することにより、暗号モジュールの利用者が、暗号モジュールのセキュリティ機能等に関する正確で詳細な情報を把握できるようにすることを目的とした制度。IPAにより運用されている。
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	クラウドコンピューティング	データサービス等が、ネットワーク上にあるサーバ群（クラウド（雲））にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」利用することができるコンピュータ・ネットワークの利用形態。
	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。

	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	経済産業省において、2011年４月策定、2014年３月改訂。経済産業省が策定した、クラウドサービス利用者及び事業者が対処すべきセキュリティマネジメントのガイドライン。
こ	国連サイバーGGE	GGE:the Group of Government Expertsの略。国連総会第一委員会のサイバーセキュリティに関する政府専門家会合。
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	2013年４月、サイバー攻撃対策の強化のため、13都道府県警察に設置された。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国際キャンペーン	2012年より毎年10月にサイバーセキュリティ国際キャンペーンを実施し、アジア、欧米をはじめとする諸国と国際連携を活用した行事やサイバーセキュリティ対策に関する情報提供を実施し、国際連携の推進と国内におけるサイバーセキュリティ対策の一層の普及を図っている。
	サイバーセキュリティ戦略	2013年６月10日、情報セキュリティ政策会議決定。「サイバーセキュリティ立国」の実現を目指し、2015年度までの３年間の国家戦略をとりまとめたもの。なお、2015年１月にサイバーセキュリティ基本法が全面施行されたことに伴い、新しい法的枠組みに基づく新たなサイバーセキュリティ戦略案をとりまとめているところであり、2015年５月25日の第２回サイバーセキュリティ戦略本部会合においてパブリックコメント案が示された。
	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。
	サイバー犯罪条約	サイバー犯罪に関しての対応を取り決めた国際条約。通称ブダペスト条約。日本においては2012年11月に効力が発生した。
	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。
し	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。
	重要インフラの情報セキュリティ対策に係る第３次行動計画	2014年５月10日情報セキュリティ政策会議決定。2015年５月25日サイバーセキュリティ戦略本部改訂。重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画。
	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３次行動計画において記載。
	情報セキュリティ研究開発戦略	2011年７月８日情報セキュリティ政策会議決定、2014年７月10日情報セキュリティ政策会議改定。

	情報セキュリティ人材育成プログラム	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・情報セキュリティ人材育成プログラムは2014年５月19日情報セキュリティ政策会議決定。
	情報セキュリティ普及啓発プログラム	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。
す	ステークホルダー	利害関係者のこと。
	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。
	スマートメーター	通信機能を有し、遠隔での検針等を行うことが可能となる新しい電力量計。
せ	脆弱性関連情報届出受付制度	2004年７月、経済産業省が「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）を公示し、脆弱性関連情報の届出の受付機関としてIPA、脆弱性関連情報に関して製品開発者への連絡及び公表に係る調整機関としてJPCERT/CCが指定されている。
	政府統一基準群	政府機関の情報セキュリティを確保するため、政府機関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情報セキュリティ政策会議決定文書等のこと。「政府機関の情報セキュリティ対策のための統一規範」（2011年４月21日情報セキュリティ政策会議決定、2014年５月19日改定）、「政府機関の情報セキュリティ対策のための統一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、2014年５月19日改定）、「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」（2005年９月15日同会議決定、2014年５月19日改定）等。
	セキュリティ・キャンプ実施協議会	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。
そ	総合科学技術・イノベーション会議	内閣総理大臣及び国務大臣と有識者の議場として、日本全体の科学技術を俯瞰し、各省より一段高い立場から、総合的・基本的な科学技術政策の企画立案及び総合調整を行うことを目的として、2001年１月に内閣府に総合科学技術会議が設置された。2014年５月、単なる研究開発の促進のみならず、その成果を産業化等の出口へ繋げてゆくことの明確化を企図し、総合科学技術・イノベーション会議に改称。
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。
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。
	テレコム・アイザック推進会議	一般財団法人日本データ通信協会 テレコム・アイザック推進会議（Telecom-ISAC Japan、ISAC：Information Sharing and Analysis Center）。国内の主要ISP等が中心となって2002年に設立された、通信サービスの安全な運用のためにサイバー攻撃関連情報の共有及び分析等を行う民間組織。
	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。
な	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。略称はNISC（National center of Incident readiness and Strategy for Cybersecurity）。
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）
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。
	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。この攻撃では、標的の組織がよくやり取りをする形式や内容の電子メールを送りつけ、その電子メールの添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する手口がよく使われている。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	コンピュータウイルス、ワーム、スパイウェア等の、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。
ほ	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。
	リバースエンジニアリング	Reverse engineering。ソフトウェアやハードウェアなどを解析・分解し、その仕組みや仕様、目的、要素技術などを明らかにすること。
	量子暗号	量子力学の理論を用いた暗号技術。原理的に盗聴の有無を検知できる特性を持つ。