資料２

サイバーセキュリティ 2017（案）

資料２－１　サイバーセキュリティ 2017（案）の概要

資料２－２　サイバーセキュリティ 2017（案）

サイバーセキュリティ2017(案)の概要について

資料２－１

サイバーセキュリティ戦略に基づく３期目の年次計画として、2017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推進コンソーシアムを通じ、IoTセキュリティガイドラインを普及【総務省及び経済産業省】
- 官民の連携による「ボット撲滅」に向けた体制構築及び対策の推進【内閣官房、関係各省】

■セキュリティマインドを持った企業経営の推進

- サイバーセキュリティ経営ガイドラインの普及【経済産業省】
- 具体的な人材育成のカリキュラム策定【内閣官房】
- 金融業界横断的な演習を実施【金融庁】
- ICT分野の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

- セキュリティサービスを認定する体制整備による競争力強化等、セキュリティの成長産業化【経済産業省】
- 著作権法におけるセキュリティ目的のコンピュータプログラムの解析（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【文部科学省】
- IoTシステムのセキュリティ認証制度にかかる評価・検討【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

- 民間の取組主体と協力し、サイバーセキュリティに関する普及啓発を実施【内閣官房】
- 大学等のセキュリティ対策の取組強化促進【文部科学省】
- 一般財団法人日本サイバー犯罪対策センターとの連携【警察庁】
- 情報共有・連携ネットワーク（仮称）の構築・運用【内閣官房、関係各省】

■重要インフラを守るための取組

- 「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」に基づく施策の実施【内閣官房及び重要インフラ所管省庁等】
- 産業サイバーセキュリティセンターにおいて、重要インフラ等におけるセキュリティ対策の中核を担う人材の育成【経済産業省】

■政府機関を守るための取組

- 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、訓練・演習を実施【内閣官房及び総務省】
- 独立行政法人・指定法人に対する監査の実施、監視業務の監督【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

- 対処機関における情報収集・分析機能及び対処能力向上【警察庁、法務省、防衛省、関係各省】
- 先端技術の防護のため、国立研究開発法人・大学等のセキュリティ対策の取組強化促進【内閣官房、文部科学省、関係各省】

■国際社会の平和・安定

- 国際的な情報発信の強化【内閣官房、外務省、関係各省】
- 国際法・規範の議論と法執行の国際連携の両面から、サイバー空間への法の支配の確立に積極的に関与【内閣官房、外務省、関係各省】
- ASEAN等における能力構築を政府一体的に支援【内閣官房、外務省、関係各省】

■世界各国との協力連携

- G7伊勢志摩サイバーグループを含め、G7各国との政策協調及び実務的な協力を強化【内閣官房、外務省】
- 二国間協議や多国間協議を通じたASEANや米国等、世界各地域のパートナーとの連携の更なる強化【内閣官房、外務省、関係各省】

横断的施策

■研究開発の推進

- 様々な社会科学的視点も含めた「サイバーセキュリティ研究開発戦略」の推進【内閣官房】
- 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を支える研究開発等の実施【経済産業省】
- 戦略的イノベーション創造プログラム（SIP）の枠組みにより、真贋判定技術を含めた動作監視・解析技術と防御技術の研究開発を行う【内閣府】

■人材の育成・確保

- 「サイバーセキュリティ人材育成プログラム」に基づく施策を促進【内閣官房】
- ナショナルサイバートレーニングセンターを通じ、若年層のICT人材を対象に、未来のサイバーセキュリティ研究者・起業家を育成【総務省】
- サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）の実施【総務省】

推進体制

- 東京オリンピック・パラリンピック競技大会を見据えた横断的リスク評価、サイバーセキュリティ対処調整センターの情報共有システムの構築　等【内閣官房】

資料２－２

サイバーセキュリティ２０１７

（案）

2017 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、様々な役割を担う多様な主体による連携のもと自律的なガバナンスの基により発展してきた。情報の自由な流通が確保されることで、民間企業を中心とした新たな創意と発想による無限の価値を産み出す場となり、人類に対して計り知れない恩恵をもたらしてきた。このように発展を続けるサイバー空間の中で流通する情報量は爆発的に増加している中、2017年５月には、ランサムウェアWannaCryによる我が国を含め世界規模でのサイバー攻撃が発生しており、近年のサイバー攻撃の激化などサイバー空間における脅威がますます高まる状況にある。このため、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・危機管理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、我が国においては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が2014年11月に成立した。政府は同法の規定に基づき、2020年東京オリンピック・パラリンピック競技大会の開催、さらにその先の2020年代初頭までを見据えつつ、サイバーセキュリティ政策の基本的な方向性を示す新たな国家戦略「サイバーセキュリティ戦略」を2015年９月４日に閣議決定した。そして、2015年度より同戦略に基づく年次計画を策定し、サイバーセキュリティに関する施策を着実に推進してきた。

本書は同戦略に基づく３期目の年次計画であり、政府が2017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である。今後、サイバー空間が一層発展することが期待されるなか、引き続き、グローバルなサイバー空間の健全な発展に向けて、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、「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（平成29年5月30日閣議決定）を踏まえ、データ利活用の促進と同時並行的に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。

(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。さらに、その確認を適時確認していく。また、「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」を踏まえつつ、官民の連携の下、安全なIoTシステムの創出に向けた取組を推進する。

(イ)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。

(3) IoTシステムのセキュリティに係る制度整備

(ア)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、IoTセキュリティの確保に向けた総合的な対策及び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。

(イ)経済産業省において、IoTシステムの構成要素であるM2M機器等の制御システム向け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評価・認証の仕組みを検討する。

(ウ)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。

(エ)経済産業省において、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により、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。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。

(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。

(イ)経済産業省において、IoTのセキュリティ対策等に関する研究開発を行う。

(ウ)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。

(エ)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、自動車のセキュリティ上の課題について、車両レベル・コンポーネントレベル、制御システム等の研究開発を推進する。

(オ)総務省において、「IoTセキュリティ対策の取組方針ver1.0」を踏まえ、既に流通している脆弱性を有するIoT機器のセキュリティ対策に取り組むとともに、今後製造するIoT機器のセキュリティ対策について検討を行う。

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)内閣官房において、関係府省庁と協力して、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」を踏まえ、企業のサイバーセキュリティに係る取組について、現状の把握を行い、さらなるサイバーセキュリティ対策の推進に関する検討を行う。

(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、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。

(ウ)経済産業省において、企業のサイバーセキュリティ対策を推進するため、サイバーセキュリティ保険など、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組を、加点要素等として考慮する仕組みなどのインセンティブ策を検討する。

(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)内閣官房において、サイバーセキュリティ人材育成プログラムを踏まえ、経営層、橋渡し人材層、実務者層など、それぞれの人材層向けのさまざまな施策について連携を強化することにより、より効果的かつ効率的に施策が進められるよう、施策間連携を図るためのワーキンググループを通じ、モデルとなる具体的な人材育成のカリキュラムの策定等を行う。

(3) 組織能力の向上

(ア)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

一の形で公開し、普及を図る。

(イ)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。

(ウ)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。

(エ)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。

(オ)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、サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）を実施する。また、2020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する。

(カ)経済産業省において、重要インフラ企業等に対するサイバー攻撃への対処能力向上のため、模擬システム等を用いた実践的なサイバー演習を行う。

(キ)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。

(ク)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を引き続き実施する。

(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。

(サ)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。

(シ)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。

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、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認定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。

(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等の普及促進を行う。

(ウ)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、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。

(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)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、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。

(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、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。

(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、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、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。

(カ)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。

(キ)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。

(ク)経済産業省において、IoTシステムセキュリティの国際標準規格を視野に入れた認証制度にかかる評価・検討を行う。

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)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。

(イ)経済産業省において、IPAを通じ、IoT機器、サービスを支える組込み産業の高度化に向け、産業動向の把握・分析を行うとともに、「セキュリティ・バイ・デザイン」の産業展開の観点から、セキュリティとセーフティ設計プロセスの整合化やシステムアプローチによるセキュリティ分析手法の検討を進め、組込みコーディングスタンダードの整備普及を図る。

(ウ)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。

(エ)経済産業省において、IPAを通じ、情報処理システムや組込みシステム等におけるソフトウェアの不具合や脆弱性が社会に与える混乱や被害を防止する観点から、企画・設計段階からセキュリティ配慮が行われるようIoTセキュリティガイドラインの普及・国際標準化の取り組みを進めるとともに、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、設計プロセス・利用時体験・流通するデータ等多面的な観点から利用者への品質説明力を強化する。

(オ)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、「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。

(カ)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。

(キ)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。

(ク)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。

(ケ)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）等を行う実証（ACTIVE）を引き続き実施する。

(コ)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。

(サ)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。

(シ)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。

(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)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。

(ソ)内閣官房及び関係省庁において、サイバー空間を安全に利用でき、また安全に発展させるよう、サイバーインシデント情報やその脅威情報を分析し、民間等の関係主体と共有することで着実にそのインシデント等への対応に繋げるため、情報共有・連携ネットワーク（仮称）の構築・運用に向けた検討を進める。

(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」の改訂を行うとともに、同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を通じ普及啓発活動を進める。

(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、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。

(エ)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。

(オ)文部科学省において、2015年度に作成した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、指導主事、教員等を対象としたセミナー及びフォーラムを実施する。

(カ)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、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。

(キ)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。

(ク)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。

(ケ)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。

(コ)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。

(サ)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。

(シ)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等のツール等の利用促進等を図る。

(ス)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。

(セ)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。

(ソ)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。

(タ)文部科学省において、大学等における多岐にわたる情報資産や多様なシステムの利用実態といった特性を踏まえ、大学等のマネジメント面・技術面の取組の強化を促進するとともに、大学等の自律的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る枠組みを整備し、これら取組を支援する。

(チ)個人情報保護委員会において、関係省庁と協力し、2017年5月30日に全面施行された改正個人情報保護法を踏まえ、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にかかる対応が適切に実施されるよう、情報セキュリティ関係機関と連携して取り組む。

(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、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犯罪被害防止のための教育等の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。

(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、全国の情報技術解析部門で効果的かつ効率的な解析を推進することにより、多様化・複雑化が著しいサイバー犯罪に的確に対処する。また、家電、電気メーター、自動車等の日常生活に近い機器に係るオンライン化等の新たな技術やサービスの開発が次々に進められている背景を踏まえ、デジタルフォレンジックに係る対処能力をより一層強化する。

(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。

(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)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、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。

(ウ)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し、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、この取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

- 迅速かつ効率的な情報共有に資するため、情報共有システム構築に係る調査検討を行う。
- 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への利活用のための「機能保証に向けたリスクアセスメント・ガイドライン」の一般化を行う。
- 事業継続計画及びコンティンジェンシープランに盛り込まれるべき要点等を整理する。
- 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の整理等を行う。

(エ)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。

(オ)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。

(カ)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、重要インフラにおけるサイバー攻撃への対処能力を向上させるための実践的サイバー防御演習（CYDER）を実施する。
- 経済産業省において、重要インフラ等企業におけるサイバー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。
- 金融庁において、金融業界横断的なサイバーセキュリティ演習を引き続き実施する。

(キ)経済産業省において、IPAに、2017年４月に「産業サイバーセキュリティセンター」を設立し、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向けて、７月に教育カリキュラムを開始する。さらに、センターにおいて、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。

(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。

(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、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判断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。
- ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）の検討を進める。

(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。

(オ)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、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や保有するシステムに対するぜい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。

(キ)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、2018年6月までの円滑な施行に向けて、政省令等の整備を進める。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、2017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-2017-」に基づく関係事業者等の取組を更に推進するとともに、進捗状況等を踏まえて、必要な見直しを行う。

(3) 各分野の個別事情への支援

(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。2016年度に作成・提供した訓練ツールを活用し、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・検知を行うとともに、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構築に係るフォローアップ及び、2017年度予算を活用し、地方公共団体の情報セキュリティ対策に係るLGWAN環境の健全性を補完する新たなプラットフォームの構築により、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、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)内閣府において、2017年7月に試行運用を開始し、2017年秋頃に本格運用を開始する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。

(キ)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、IPAとJPCERT/CCと連携し、制御システムに係る脆弱性情報の提供収集・分析・展開にも取り組む。

(ク)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、セキュリティ対策に関する知見を収集し、それに基づいた実践的な演習を実施する。

(ケ)経済産業省において、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、制御システムのセキュリティに関する評価・認証制度の検討を行う。

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、統一基準群を始めとした規程に適時反映するため、統一基準群の次期改定に向けた検討を進める。

(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。

(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、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、情報システムの調達仕様書の策定段階において適切に定めるべきセキュリティ対策要件について検討を行い、各府省庁におけるセキュリティ・バイ・デザインの取組を促進する。また、各府省庁共通的に取り組むべき事項については、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手順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、各府省庁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行い、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。

(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、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とともに、将来のGSOCシステムにおける監視の在り方を検討する。

(コ)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更なる検討を行う。

(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・対処機能が強化されるよう、CSIRT体制の強化やインシデント対処の改善に関する各府省庁の取組状況及び課題を把握し、府省庁CSIRTの対処能力の更なる強化のために必要な施策を検討する。

(シ)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、独立行政法人及び指定法人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の実施を検討する。
- 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、政府機関におけるサイバー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、政府機関のインシデント対処能力の向上のため、府省間の競技形式による演習（NATIONAL 318(CYBER) EKIDEN）を実施する。

(ス)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。

(セ)内閣官房において、政府職員のインシデント対処能力等を向上させていくため、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、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。

(タ)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。

(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、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年間で全府省庁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。2017 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・システムを対象とした内容とした監査テーマで実施する。

(イ) 内閣官房及び各府省庁において、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、「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」の推進を始めとし、体制の整備、有意な人材の確保、一定の専門性を有する人材の育成、適切な処遇の確保を含む政府内部のセキュリティ人材の充実に係る諸施策を推進する。

(ウ) 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。

(エ) 内閣官房において、引き続き、府省庁、独立行政法人及び指定法人を対象に、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。

(オ) 内閣官房及び総務省において、各府省庁のセキュリティ・IT 人材の育成・確保のため、現行の研修体系の抜本的整理を進めるとともに、研修修了者にスキル認定を行う枠組みを構築し、研修修了者等に対するスキル認定の実施に向けて取り組む。

(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、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、各府省庁と共有し、統一的な対策の必要性が把握された場合は統一基準群等への反映に向けた検討を行う。

(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、IPAとの連携等により、引き続き、日本年金機構を含む独立行政法人・指定法人に対して監査を行う。監査の実施に当たっては、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し監査を行う計画とする。また、IPAの実施する、独立行政法人・指定法人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。

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)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)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・分析する体制を強化するとともに、必要な機材の拡充を実施する。

(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、大規模産業型制御システムに対するサイバー攻撃及び当該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、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。さらに、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)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。

(カ)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。

(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)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、次年度の実施に向けた所要の準備を進める。

(ケ)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。

(2) 我が国の先端技術の活用・防護

(ア)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。

(イ)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について、当該法人のマネジメント・技術面の取組を促進するとともに、これら法人相互の協力による自立的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る支援を本格化させる。
- 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) 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、任務遂行上依拠する社会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)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。

(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、経済産業省及び防衛省において、各二国間協議や国連政府専門家会合、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)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/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。

(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、関係府省庁が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、サイバー空間における国際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)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情報セキュリティ政策会議を通じた人材育成の取組や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）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、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２回日・ASEANサイバー犯罪対策対話や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。

(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、我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)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。

(イ)内閣官房及び外務省において、サイバー空間の安全及び安定を促進するため、「Ｇ７伊勢志摩サイバーグループ」を含め、Ｇ７各国との政策協調及び実務的な協力の強化に向け、Ｇ７各国と連携のうえ我が国も引き続きイニシアチブを発揮していく。

(ウ)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。

(エ)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。

(オ)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。

(カ)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。

(キ)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。

(ク)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。

(ケ)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。

(コ)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。

(1) アジア大洋州

(ア)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、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。さらに、ARFを中心とした地域の枠組みによる信頼醸成を進める。

(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、オーストラリアとのサイバー防衛協力を推進

していく。

(2) 北米

(ア)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。

(イ)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。

(ウ)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。

(3) 欧州

(ア)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、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。

(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、JEDSと定期的に協議を行う。

(4) 中南米、中東アフリカ

(ア)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、二国間協議を実施していない国との関係も強化する。

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た「サイバーセキュリティ研究開発戦略」を策定する。

(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確保する上で、さまざまなシステムで利用されている暗号方式・プロトコル等の安全性評価を行い、システムの安全性維持に向けた研究開発を実施する。

(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、政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術の研究開発を行う。また、サイバーセキュリティ関連情報の大規模集約を行うとともに、セキュリティ検証プラットフォームを構築し、サイバーセキュリティ研究の基盤となる環境整備を行う。

(イ)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。

(ウ)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。

(エ)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。

(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、信頼性工学、心理学等の様々な社会科学的視点も含めた「サイバーセキュリティ研究開発戦略」を策定する。

(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、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。

(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。

(イ)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、暗号プロトコル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、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。

(ウ)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。

(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。

(5) 関係機関との連携

(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）「重要インフラ等におけるサイバーセキュリティの確保」により真贋判定技術（機器やソフトウェアの真正性・完全性を確認する技術）を含めた動作監視・解析技術と防御技術の研究開発を行う。

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、「サイバーセキュリティ人材育成プログラム」に基づき、施策間連携を図りつつ、関係施策を促進していく。

(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、産業界や大学、関係省庁等、産学官の連携体制の下、情報共有を行いつつ、モデルとなるカリキュラムの策定をはじめとした施策間連携を推進する。

(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。また、並行して、2016年より、情報セキュリティ教育の演習拠点を整備（2016年：５拠点、2017年：５拠点（予定)、合計10拠点整備予定）し、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)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。

(カ)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。

(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、次期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。

(イ)文部科学省において、教員研修センターと連携し、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。また、教員等を対象とした情報モラル教育セミナー・フォーラム等を開催する。

(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 2017」）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」の普及を図る。

(ウ)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。

(エ)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）制度の着実な実施に向けて必要な措置を講じるとともに、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。

(オ)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、未来のサイバーセキュリティ研究者・起業家の育成に取り組む。

(5) 組織力を高めるための人材育成

(ア)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。

(イ)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、独立行政法人、重要インフラ事業者及び地方公共団体等におけるサイバー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サイバー防御演習（CYDER）を実施する。

(ウ)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。

(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取組を実施する。また、任務保証の観点から、任務遂行上依拠する社会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。

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の一層の進化を図るため、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。中期的には、2020年東京オリンピック・パラリンピック競技大会を見据え、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)警察庁において、「セキュリティ情報センターについて」(2015年８月３日セキュリティ幹事会決定）等に基づき、セキュリティ情報センターを設置する。同センターにおいては、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。

(ウ)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のため、運営に大きな影響を及ぼし得る重要サービス事業者等におけるサイバーセキュリティに係るリスク評価について、大会の詳細や情勢の変化に応じた手順書の見直しを実施するとともに、地方における会場等を勘案し、対象となる事業者の地理的、分野的な拡大を図る。更に、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していく。また、これら重要サービス事業者等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サイバーセキュリティ対処調整センター（オリンピック・パラリンピックCSIRT）の2018年度中の構築に向け、情報共有システムの構築を推進するとともに、2018年２月から３月にかけて開催される平昌冬期オリンピック・パラリンピック競技大会等の機会をとらえ関係組織間のさらなる連携の深化を図る。

(エ)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。

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。
	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。
	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。
	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。
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か国の官・民・大学等321の組織が参加している。
G	G7/G8	Group of Seven（主要７か国首脳会議）、Group of Eight（主要８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。政府機関に設置したセンサー（GSOC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。
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。あらゆるモノ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。
	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。
	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か国）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。
	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か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 Subgroup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JIWG傘下の検討部会。
	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）Working Group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JIWG傘下の検討部会。
	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」を目指す我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	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 CTF2017	SECCON CTF：SECurity CONtest Capture The Flag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。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。
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。
U	UNODC	United Nations Office on Drugs and Crimeの略。国連薬物・犯罪事務所。
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ィア等から、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）。機密性、完全性、可能性は情報セキュリティの三大要素と呼ばれている。
	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）。機密性、完全性、可能性は情報セキュリティの三大要素と呼ばれている。
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）。機密性、完全性、可能性は情報セキュリティの三大要素と呼ばれている。

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。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。
	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。
	クラウドセキュリティガイドライン活用ガイドブック	経済産業省において、2014年３月に、「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」改訂版と併せて公表した、同ガイドラインの解説書。
こ	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	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。国による監視、監査、原因究明調査の対象範囲を独立行政法人等にも拡大する改正法が、2016年４月15日に可決・成立し、同月22日に公布。
	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人材育成総合強化方針	2016年３月31日サイバーセキュリティ戦略本部決定。「「日本再興戦略」改訂2015」（2015年６月閣議決定）、「サイバーセキュリティ戦略」（2015年９月４日閣議決定）等を踏まえ、サイバーセキュリティ分野の人材育成の具体的な強化方針を示したもの。
	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	2015年９月４日、閣議決定。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、2020年代初頭までの将来を見据えつつ、今後３年程度の基本的な施策の方向性を示したもの。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、新たな法的枠組みに基づき策定された。
	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。
	サイバー犯罪に関する条約	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。我が国においては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	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）。
	情報セキュリティ事象	情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。（JIS Q 27000:2014）
	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。
	新・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。2014年７月10日情報セキュリティ政策会議決定。
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。

	セキュリティ・バイ・デザイン	情報システムのライフサイクル（企画・設計・開発・運用・廃棄）に関して、企画・設計段階から情報セキュリティの観点を意識し、その際に必要となる調達仕様にセキュリティ要件を適切に組み込むこと。
	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。
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。
	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。
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。
	標的型メール	標的型攻撃を参照。
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	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	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、「インターネットリテラシー」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。