資料５－２

サイバーセキュリティ２０１４
【案】

２０１４年７月　　日

情報セキュリティ政策会議

目　次

はじめに

ICT に大きく依存している現代社会において、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はもとより、国家の安全保障・危機管理においても極めて重要な課題となっている。一方、政府機関や企業の機密情報の窃取を意図した標的型攻撃、国民生活や社会経済活動に直結する重要インフラ等の制御システムを狙った攻撃、急速に普及したスマートデバイス等を介した大規模な個人情報の窃取など、サイバー攻撃の態様は一層複雑化・巧妙化してきている。

内閣官房長官を議長とする情報セキュリティ政策会議は、このようにサイバー空間と実空間の融合・一体化が進み、サイバー空間を取り巻くリスクが一段と深刻化している現状に対応すべく、昨年６月、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。）を策定した。

戦略は 2015 年までの３年間を対象とした取組を掲げており、内閣官房情報セキュリティセンター（以下「NISC」という。）を結節点として、政府機関等や重要インフラ事業者等の各主体が相互に連携しつつ、セキュリティ水準の向上やサイバー攻撃への対処能力の強化などに関する取組を推進することを通して、世界を率先する強靭で活力あるサイバー空間を構築し、もって「サイバーセキュリティ立国」を実現することを目標としている。本書は同戦略に基づく２期目の年次計画であり、各府省庁が 2014 年度に実施する様々な具体的取組について、戦略記載の体系に沿ってその詳細を示すものである。

なお、本書の記載にかかわらず、サイバーセキュリティを取り巻く環境に変化が生じた場合や、2020 年東京オリンピック・パラリンピックに向けた対策の検討の進捗によっては、その内容に応じ、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 「強靱な」サイバー空間の構築

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

2014 年度においては、「政府機関統一基準群」の全面改定、「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」の策定、「情報セキュリティ普及・啓発プログラム」の改定等を踏まえて、各施策の取組をより具体化し、政府機関・独立行政法人等、重要インフラ事業者、企業・一般個人、各主体におけるセキュリティ水準の更なる向上、連携の強化を図る。

① 政府機関等における対策

1） 情報及び情報システムに係る情報セキュリティ水準の一層の向上

【 情報の重要度等に応じた政府機関における統一的な仕組みの強化 】

（ア）業務・情報の特性に応じた対策の重点実施のための枠組みの構築・運用 （内閣官房及び全府省庁）

a) 内閣官房において、各府省庁の CISO がガバナンス機能を発揮し、標的型攻撃を始めとした高度サイバー攻撃の標的となる蓋然性が高い業務を特定してリスク評価を行い、限られた人員・予算の中で重要な業務・情報を守るために必要な情報セキュリティ対策を計画的・重点的に実施するための枠組みを構築するとともに、各府省庁における適切な運用を推進する。

b) 内閣官房において、各府省庁が策定する対策推進計画により、当該府省庁の情報セキュリティに関する全体方針や取組の重点を確認し、PDCA サイクルの適正性やガバナンス機能の有効性の維持・向上を図る。

（イ）政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し （内閣官房及び全府省庁）

内閣官房において、政府機関統一基準群の改定を受けた各府省庁の情報セキュリティポリシーの見直しについて、その進捗状況の把握や支援等を行う。

（ウ）政府情報システム管理データベースの利活用 （内閣官房、総務省及び関係府省庁）

a) 内閣官房において、各府省庁の情報システムを管理するために情報資産台帳をデータベース化した「政府情報システム管理データベース」を用いて政府全体を通じたリスク管理、脆弱性の検出等への利活用を図る。

b) 総務省において、同データベースを引き続き維持・管理する。

(エ)「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の推進 （内閣官房及び関係府省庁）

各関係府省庁において、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン[1]」に基づき導出したリスク評価及び保証レベルの総合的な妥当性を確保するため、内閣官房が開催する最高情報セキュリティアドバイザー等連絡会議等の場において、専門的知見を有する者からの助言等を受け、認証方式を決定するとともに、業務・システム最適化に係るものは、計画への反映状況について、各府省情報化統括責任者（CIO）連絡会議等に報告する。

(オ) 特定秘密を取り扱うシステムに係る情報セキュリティ対策 （内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、特定秘密を取り扱うシステムに係る情報セキュリティ対策を法律施行までに取りまとめ、法律施行後は、当該対策を着実に推進する。

(カ) 特別管理秘密を取り扱うシステムに係る情報セキュリティ対策 （内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、「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[2]」に基づく特別管理秘密に係る基準を踏まえた対策の実施状況の重層的なチェックを着実に推進する。

(キ) 特に機密性の高い情報を取り扱う政府機関の情報保全システムの強化に向けた取組の推進 （内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、「特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について[3]」等を踏まえた取組を着実に推進する。

【 多様化する就労形態等への対応の強化 】

(ク) 政府機関におけるスマートフォン等の情報セキュリティ対策の強化 （内閣官房）

内閣官房において、マニュアル等を整備するなどにより、各府省庁における私物のスマートフォン等を外出先やテレワーク等で業務利用する際の情報セキュリティ対策の実施手順の作成を支援する。

【 政府横断的な情報システムの対策強化等 】

(ケ) 政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化 （内閣官房及び総務省）

a) 総務省において、「政府共通プラットフォーム」の円滑な運用を行うとともに、高度化

---

[1] 2010年8月31日各府省情報化統括責任者（CIO）連絡会議決定。
[2] 2007年8月9日カウンターインテリジェンス推進会議決定。
[3] 2011年7月1日情報保全システムに関する有識者会議（政府における情報保全に関する検討委員会（委員長:内閣官房長官）の下で開催された有識者会議）決定。

する情報セキュリティ上の脅威に的確な対応を実施する。

b) 内閣官房において、同プラットフォームにおける情報セキュリティ対策について、政府機関統一基準群の改定その他の関連施策により蓄積された専門的知見を提供するなどの支援を実施する。

(コ) 複数の府省庁で共通的に使用する政府情報システム基盤の運用管理に関する体制等の整備 （内閣官房、総務省及び全府省庁）

総務省及び各府省庁において、「政府共通プラットフォーム」及び同プラットフォームへの統合・集約化対象システムについて、各府省庁の責任と役割分担、平常時及び非常時の協力・連携体制、非常時における具体的な対応策等を定めた運用管理基本規程等の規程類に基づき、適切に運用管理を行う。

(サ) 社会保障・税番号制度に対応した情報セキュリティ対策 （内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、関係機関が管理・運用する情報提供ネットワークシステム等の構築にあたって、適切な個人情報保護及び情報セキュリティの確保を図る。具体的には、①個人情報を一元管理せず分散管理、②情報提供ネットワークシステムを用いた情報連携において個人番号ではなく符号を利用、③アクセス制御によりシステム内の特定個人情報にアクセスできる人を制限、④通信を暗号化、などの対策を講じる。

(シ) オープンデータ推進における情報セキュリティの確保 （内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、機械判読に適したデータ形式での公開やデータカタログの整備など電子行政オープンデータに関する具体的な取組を推進するに当たり、十分な情報セキュリティの確保を図る。

【 情報システムにおけるサプライチェーン・リスク等への対応強化 】

(ス) 情報システムに企画・設計段階から情報セキュリティ対策が適切に組み込まれるための方策 （内閣官房、総務省及び全府省庁）

a) 各府省庁において、システム予算全体の中で必要な情報セキュリティ対策を確保できるよう、あらかじめ可能な限りの想定を行い、それぞれの情報システムに係る調達仕様書の作成において、必要なセキュリティ対策を確実に記載するため、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル[4]」を活用する。

b) 内閣官房において、同マニュアルが情報システムに係る政府調達で広く活用されるよう、本マニュアルの利便性・簡便性の向上、内容の充実や、各府省庁における普及・利用の促進を図るなどの取組を行う。また、各府省庁の調達書における活用状況を調査するとともに、問合せ対応や作業支援等を実施する。

[4] 2011年3月30日情報セキュリティを企画・設計段階から確保するための方策に係る検討会とりまとめ。

(セ) 調達時における対策の推進 （内閣官房）

内閣官房において、サプライチェーン・リスクへの対応に関する情報収集等を行い、各府省庁と情報を共有するなどにより、政府機関統一基準群における関連規定の適切な運用を図る。

(ソ) 安全性・信頼性の高い IT 製品等の利用推進 （経済産業省及び全府省庁）

a) 各府省庁において、安全性・信頼性の高い情報システムを構築するため、IT 製品等を調達する際には、政府機関統一基準群に基づき、「IT 製品の調達におけるセキュリティ要件リスト[5]」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定し、適切な機器を調達する。

b) 経済産業省において、各府省庁が情報セキュリティに配慮した IT システムの調達を実効的かつ効率的に行えるようにするため、IPA が運営する JISEC 認証製品の活用推進のため、本リストの必要に応じた見直しなどにより、政府機関等における活用を促進する。

(タ) 政府調達における情報セキュリティの確保 （内閣官房及び経済産業省）

a) 経済産業省において、政府調達等における情報セキュリティの確保に資するため、IPA を通じ、政府及び地方公共団体の調達担当者等に対して、政府機関統一基準群を遵守するように、「IT 製品の調達におけるセキュリティ要件リスト」の要件を満たす認証取得製品等の情報提供や普及啓発を行うとともに、政府、地方公共団体及び民間企業における同リストの有効活用のため必要な情報をガイドブックとしてまとめて提供する。

b) 経済産業省において、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）についての定期的な見直し及び最新のプロテクション・プロファイル（翻訳版）の情報提供を行う。

c) 経済産業省において、IPA を通じ、JISEC 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。

(チ) 情報システムの設計等の段階における情報セキュリティの技術基準の整備等 （内閣官房及び全府省庁）

内閣官房において、政府機関の情報システムについて、特に標的型攻撃から重要な業務や情報を守る観点で情報システムの設計、構築、運用等の段階について満たすべき情報セキュリティの技術基準を検討、整備し、各府省庁における適切な運用を図る。

(ツ) 運用・管理を委託している情報システムの情報セキュリティ対策の強化 （内閣官房）

内閣官房において、クラウドコンピューティングを含む運用・管理を外部に委託している政府機関の情報システムについて、情報セキュリティを確保するための取組を推進する。

---

[5] 経済産業省及び IPA にて 2014 年 1 月パブリックコメント実施。

【 安全な暗号利用の推進 】

(テ) 政府機関における安全な暗号利用の推進 （内閣官房、総務省、経済産業省及び全府省庁）

a) 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。

b) 総務省及び経済産業省において、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。

c) 内閣官房において、必要に応じて、CRYPTREC 暗号リストに掲載された暗号技術の監視により得られた情報を総務省及び経済産業省から提供を受け、必要な情報を速やかに各府省庁に提供する。また、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針[6]」に基づく各府省庁の取組を推進する。

(ト) 安全性・信頼性の高い暗号モジュールの利用推進 （経済産業省及び全府省庁）

a) 経済産業省において、安全性の高い暗号モジュールを利用するため、IPA の運用する暗号モジュール試験及び認証制度（JCMVP）を推進する。

b) 各府省庁において、暗号モジュールを調達する際には、必要に応じて、同制度により認証された製品等を取り扱う。

【 電子メールに係るなりすまし防止等の対応強化 】

(ナ) 政府機関から発信する電子メールに係るなりすましの防止 （内閣官房、総務省及び全府省庁）

a) 内閣官房において、悪意の第三者が政府機関又は政府機関の職員になりすまし、一般国民や民間企業等に害を及ぼすことがないよう、全府省庁における送信側及び受信側における送信ドメイン認証技術（SPF、DKIM 等）等の導入を推進する。

b) 総務省において、迷惑メール対策に関わる関係者が幅広く参加し設立された「迷惑メール対策推進協議会」や、国内の主要インターネット接続サービス事業者や携帯電話事業者等と連携して、送信側及び受信側における送信ドメイン認証技術（SPF、DKIM 等）等の導入を促進する。

(ニ) 政府機関のドメイン名であることが保証されるドメイン名の使用の推進 （内閣官房、総務省及び全府省庁）

内閣官房及び総務省において、政府機関が国民に対して情報の発信を行う際に利用するドメイン名については、原則として政府機関であることが保証されるドメイン名（属性型 JP ドメイン名のうち「.GO.JP」ドメイン名）の利用を徹底するよう各府省庁に対して促す。

---

[6] 2008 年 4 月 22 日 情報セキュリティ政策会議決定。2012 年 10 月 26 日改定。

(ヌ) 政府認証基盤を活用した電子署名の利用等の推進 （内閣官房及び全府省庁）

内閣官房において、関係府省庁と協力し、政府認証基盤（GPKI）を活用した電子署名の利用等により、政府機関において公開している電子ファイルの正当性・安全性の担保に資するための取組を実施する。

【 国の重要な情報を取り扱う企業等における対策の強化 】

(ネ) 国の重要な情報を扱う企業等の情報セキュリティ対策の推進 （内閣官房及び全府省庁）

a) 各府省庁において、国の安全に関する重要な情報を扱う契約を締結する際には、「調達におけるセキュリティ要件の記載について[7]」を踏まえ、情報セキュリティ要件を定め、これを遵守するよう、契約の相手方に求める。

b) 内閣官房において、各府省庁と協力し、重要インフラ分野等における取組を参考にしつつ、国の安全に関する重要な情報を扱う企業等によるサイバー攻撃に関するインシデント情報の発注元省庁等への報告及び事業者間の情報共有を推進するとともに、政府機関におけるリスク評価手法の運用にも活用できる枠組みについて2013年度に検討した結果に基づいて、施策を推進する。

【 独立行政法人、地方公共団体等における対策の強化 】

(ノ) 独立行政法人等における情報セキュリティ対策の推進 （内閣官房、独立行政法人等所管府省庁及び関係府省庁）

a) 内閣官房において、独立行政法人等を所管する府省庁と協力し、独立行政法人等においても政府機関統一基準群を始めとした政府機関における取組を踏まえ、情報セキュリティポリシーの策定等及びそれに基づく対策の着実な実施がなされるよう取組を推進する。

b) 関係府省庁において、独立行政法人等における情報セキュリティ対策の推進を図るとともに、中期目標に情報セキュリティ対策に係る事項を明記することを推進する。

(ハ) 地方公共団体の情報セキュリティ対策水準向上のための普及・啓発 （総務省）

a) 総務省において、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。

b) 総務省において、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。

c) 総務省において、Web サーバ等公開サーバやネットワーク機器等における脆弱性診断を

[7] 2012年1月内閣官房副長官通知。

希望する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。

d) 総務省において、閲覧しただけで感染する Web 感染型マルウェアによる改ざん検知を希望する地方公共団体に対して実施する。関連のセミナーを全国５カ所で開催する。また、標的型攻撃の検知についても希望する団体に対して実施し、防御を支援する。

e) 総務省において、地方公共団体から発信する電子メールについて、悪意の第三者が地方公共団体又は地方公共団体の職員になりすまし、一般国民や民間企業等に害を及ぼすことがないよう、SPF、DKIM 等の送信ドメイン認証技術の採用等を推進する。

2) サイバー攻撃への対処態勢の充実・強化

【 GSOC の抜本的強化 】

(ア) 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の運用による緊急対応能力の向上 （内閣官房及び全府省庁）

a) 内閣官房において、全府省庁と協力し、2008 年度に本格運用を開始し、政府機関情報システムの 24 時間監視を行っている GSOC で収集・分析したサイバー攻撃等に関する情報について、速やかに情報共有を進めるとともに、関係機関との連携を通じて、政府全体として緊急対応能力の向上を図る。

b) 内閣官房において、全府省庁と協力し、訓練等を通じて緊急時の連絡体制を確認し、実効性を確保する。

c) 内閣官房において、政府情報システムの集約化の進捗状況を踏まえ、GSOC の監視対象先を拡大するための方策を検討し、着手可能な組織から監視対象の拡大を実施するとともに、監視対象先におけるサイバー攻撃等のインシデント情報の効果的な収集及び高度な解析を行うための技術の採用や人員の配置等について 2013 年度の検討結果に基づき、GSOC の態勢を強化する。

また、監視対象先からのインシデント情報の収集機能及び高度な解析機能については、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組と合わせて強化するための方策について検討を継続し、結論を得る。

(イ) サイバー攻撃事態への対処に資する情報の集約・共有の充実 （内閣官房及び全府省庁）

内閣官房において、政府機関等に対するサイバー攻撃に関する全般的な傾向や情勢について分析を行い、各政府機関に対して当該分析結果を定期的に提供する。

【 CYMAT と CSIRT 等との連携強化や訓練等による対処態勢の構築・強化 】

(ウ) 情報セキュリティ緊急支援チーム（CYMAT）要員等への訓練による対処能力の向上 （内閣官房及び全府省庁）

内閣官房において、各府省庁と協力し、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。

(エ) CSIRT 等の体制の整備及び連携の強化 （内閣官房及び全府省庁）

内閣官房において、訓練等を実施し、各府省庁の CSIRT 等の機能の維持・向上、各府省庁の CSIRT 等相互間の連携強化等を推進する。

(オ) 公開ウェブサーバに対する脆弱性検査の実施 （内閣官房及び関係府省庁）

内閣官房において、各府省庁との協力の下、希望府省庁の主要な公開ウェブサーバに対す

る脆弱性検査を実施し、その結果を当該府省庁等にフィードバックする。また、得られた知見については、全府省庁等で共有し、その成果を公表するとともに、次年度における重点検査の検査項目に適宜反映することで政府機関全体の対策状況の底上げを図る。

(カ)「新たなサイバー攻撃に対する情報セキュリティ防御モデル」の検討及び演習の実施（総務省）

総務省において、引き続きサイバー攻撃の解析及び防御モデルの検討を行い、官民参加型の実践的な防御演習を行う。

(キ) 大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等 （内閣官房及び関係府省庁）

内閣官房において、関係府省庁と協力し、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を実施し、当該結果を踏まえた検討を行うこと等により、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について[8]」、「大規模サイバー攻撃事態等への初動対処について[9]」等に基づき官民が連携して的確な対応を行うことができる態勢を整備する。また、上記訓練は 2015 年度以降も継続して実施する。

(ク) 政府機関における業務継続能力の強化 （内閣官房及び全府省庁）

a) 内閣官房において、各府省庁と協力し、各府省庁の情報システム運用継続計画の運用及び維持・改善を目的に、計画策定・改善の事例や対処要件等の情報提供を行うほか、各府省庁の計画の運用及び維持・改善の状況を把握する。

b) 各府省庁において、業務継続計画を踏まえつつ、内閣官房において策定した「中央省庁における情報システム運用継続計画ガイドライン[10]」を活用して、災害や障害発生時における行政の継続性を確保する観点から、自府省庁の情報システム運用継続計画について、必要に応じて見直しを行う。

(ケ) 平時からの情報共有体制の構築 （内閣官房、総務省、経済産業省及び全府省庁）

内閣官房、総務省及び経済産業省において、各府省庁と協力し、民間の CSIRT や SOC 事業者の団体をはじめとする、情報セキュリティ関連の事業者団体等との日常的な意見交換等により、官民による情報共有を推進する。

(コ) 国際的なセキュリティカンファレンスへの参加等を通じた対処能力の向上 （内閣官房）

内閣官房において、国際的なセキュリティカンファレンスへの参加等を通じて、最先端のサイバー攻撃及びこれへの対処に関する情報収集を行い、我が国の対処能力の向上を図る。

【 人材の確保・育成 】

[8] 2003 年 11 月 21 日閣議決定。
[9] 2010 年 3 月 19 日内閣危機管理監決裁。
[10] 2011 年 3 月情報セキュリティセンター作成。2013 年 6 月改定。

(サ) 情報セキュリティに関する政府人材の育成 （内閣官房及び関係府省庁）

サイバー攻撃に関するインシデントの情報等の集約、国内外の情勢の分析、技術動向の分析が可能な内部人材の育成・採用を進めていく。

(シ) 採用時における情報セキュリティ関連素養の確認 （内閣官房及び関係府省庁）

各府省庁において、国家公務員採用に際して、情報セキュリティに関する素養の確認に努める。

(ス) 政府職員に対する教育・意識啓発の推進 （内閣官房、人事院、総務省及び全府省庁）

a) 総務省において、内閣官房と連携し、政府職員（一般職員、幹部職員及び情報セキュリティ対策担当職員）向けの統一的な教育を引き続き実施する。

b) 内閣官房において、各府省庁の情報セキュリティ担当者等を対象とした勉強会を開催するなど、政府職員の技術・知見等の向上を図る。また、情報セキュリティ対策上の役割等に応じた教材のひな形や啓発資料を作成し、各府省庁における教育等を支援する。

c) 内閣官房において、教材作成を支援するなどにより各府省庁における新規採用職員への教育機会の付与に協力するとともに、人事院において、政府職員に対する採用時の合同研修において情報セキュリティに係る内容を盛り込むなど教育機会の付与に努める。

d) 各府省庁において、CSIRT 要員等に対するインシデント対応訓練を始めとした教育・訓練を実施するなど、職員の技術・知見等の向上を図る。また、電子政府利用促進週間、情報セキュリティ月間等の機会において、情報セキュリティインシデントの事例等を踏まえた意識啓発を行う。

(セ) 人事ローテーションの工夫 （内閣官房及び関係府省庁）

各府省庁において、情報セキュリティ担当部署と NISC で人事交流を行うなど、職員の希望も踏まえつつ、情報セキュリティ担当者が長い間情報セキュリティに係る業務に携われるよう、人事ローテーションの工夫を図る。

(ソ) 優秀な外部人材の活用 （内閣官房及び関係府省庁）

内閣官房において、優秀な外部人材の活用に関する事例を収集し、情報提供を行うなど、各府省庁と協力し、官民の人事交流等により情報セキュリティに係る外部人材の活用を進める。

【 カウンターインテリジェンス 】

(タ) 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・共有に係る取組の推進 （内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、「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、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を集約するとともに当該情報について分析し、その結果を各府省庁に提供し、共有を図る。

3) その他

(ア) 情報セキュリティガバナンスの機能強化に向けた取組 （内閣官房及び全府省庁）

a) 内閣官房において、各府省庁と協力し、各府省庁の最高情報セキュリティ責任者（官房長等）等で構成する情報セキュリティ対策推進会議の場を活用して政府機関における連携の強化を図るとともに、最高情報セキュリティ責任者の指揮の下、各府省庁において組織全体の情報セキュリティ対策を一層推進するための体制の充実を図る。

b) 内閣官房において、情報セキュリティ対策推進会議の下に設置された最高情報セキュリティアドバイザー等連絡会議を逐次開催し、共通する課題に対する専門的な見地からの助言や意見・情報交換等を通じて、各府省庁の情報セキュリティに関する取組の推進を図る。

(イ)「情報セキュリティに係る年次報告書（仮）」に係る取組の推進 （内閣官房及び全府省庁）

a) 各府省庁において、自府省庁の情報セキュリティ対策を総合的に推進するための計画を策定する。

b) 内閣官房において、各府省庁における対策の実施状況について、対策実施状況報告及び重点検査を基に客観的に比較可能な形で点検し、必要な対策の実施を求める。

c) 内閣官房において、政府機関を取り巻く情報セキュリティに関する脅威とその分析等を行い、年次報告として取りまとめる。また、当該年次報告については、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすためのものとして、情報セキュリティの維持・確保にも配慮しつつ公表する。

(ウ) 情報セキュリティ対策に関連する独立行政法人等との連携の強化 （内閣官房、総務省及び経済産業省）

内閣官房において、NICT、AIST 及び IPA との間で締結した協力覚書に基づき、情報セキュリティに係る研究者・実務家の知見を蓄積・活用するなど、情報セキュリティ対策に関連する独立行政法人等との連携を強化し、政府機関統一基準群等の施策に反映する。

(エ) 独立行政法人等との緊急時等の連絡体制の整備 （内閣官房及び独立行政法人等所管府省庁）

内閣官房において、各府省庁と協力し、独立行政法人役員レベル等にもインシデント情報及び対応状況が周知されるなど実効性のあるインシデント情報共有体制を構築する。

(オ) 行政機関以外の国の機関との連携 （内閣官房）

内閣官房において、国の機関で共通する情報セキュリティ上の課題に適切に対応するため、情報セキュリティ対策推進会議や最高情報セキュリティアドバイザー等連絡会議等の場を活用するなどして、行政機関以外の国の機関との情報交換や連携を積極的に行う。

② 重要インフラ事業者等における対策

【 安全基準等の整備及び浸透 】

(ア)「安全基準等の整備及び浸透」に関する内閣官房の施策 (内閣官房)

a) 2014 年度に指針の改定に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表する。

b) 必要に応じて社会動向の変化及び新たに得た知見に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表する。

c) 上記 a)・b)を通じて、各重要インフラ分野の安全基準等の継続的改善を支援する。

d) 重要インフラ所管省庁の協力を得つつ、各重要インフラ分野における安全基準等の継続的改善状況を把握するための調査を実施し、結果を公表する。

e) 重要インフラ所管省庁の協力を得つつ、安全基準等の浸透状況等の調査を実施し、結果を公表する。

(イ)「安全基準等の整備及び浸透」に関する重要インフラ所管省庁の施策 (重要インフラ所管省庁)

a) 指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供する。

b) 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて、安全基準等の改定を実施する。

c) 重要インフラ分野ごとの安全基準等の分析・検証を支援する。

d) 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透を実施する。

e) 内閣官房が実施する安全基準等の継続的改善状況の把握に協力する。

f) 内閣官房が実施する安全基準等の浸透状況等の調査に協力する。

【 情報共有体制の強化 】

(ウ)「情報共有体制の強化」に関する内閣官房の施策 (内閣官房)

a) 平時及び大規模 IT 障害対応時の情報共有体制の運営を通じた更なる促進及び必要に応じた見直しをする。

b) 重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供をする。

c) 重要インフラ所管省庁の協力を得つつ、各セプターの機能、活動状況等を把握するための定期的な調査・ヒアリング等を実施する。

d) 先進的なセプターの機能や活動の紹介をする。

e) セプターカウンシルに参加するセプターと連携しつつ、セプターカウンシルの運営及び活動に対する支援を実施する。

f) セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境を整備する。

g) 必要に応じてサイバー空間関連事業者との連携を個別に構築し、IT 障害発生時に適時適切な情報提供を実施する。

(エ)「情報共有体制の強化」に関する重要インフラ所管省庁の施策 (重要インフラ所管省庁)

a) 内閣官房と連携しつつ、情報共有体制を運用する。

b) 重要インフラ事業者等との緊密な情報共有体制を維持する。

c) 重要インフラ事業者等からの IT 障害に係る報告の内閣官房への情報連絡をする。

d) 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力をする。

e) セプターの機能充実への支援をする。

f) セプターカウンシルへの支援をする。

g) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

(オ)「情報共有体制の強化」に関する情報セキュリティ関係省庁の施策 (情報セキュリティ関係省庁)

a) 内閣官房と連携しつつ、情報共有体制を運用する。

b) 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡をする。

c) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

(カ)「情報共有体制の強化」に関する事案対処省庁の施策 (事案対処省庁)

a) 内閣官房と連携しつつ、大規模 IT 障害対応時における情報共有体制を運用する。

b) 被災情報、テロ関連情報等の収集をする。

c) 内閣官房に対して、必要に応じ情報連絡を実施する。

d) セプターカウンシル等からの要望があった場合、意見交換等を実施する。

【 障害対応体制の強化 】

(キ)「障害対応体制の強化」に関する内閣官房の施策 (内閣官房)

a) 他省庁の IT 障害対応の演習・訓練の情報を把握し、連携の在り方を検討する。

b) 重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプタ

ーの情報疎通機能の確認（セプター訓練）等の機会を提供する。

c) 分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施する。

d) 分野横断的演習の改善策を検討する。

e) 分野横断的演習の機会を活用して、リスク分析の成果の検証並びに重要インフラ事業者等が任意に行う IT 障害発生時の早期復旧手順及び IT-BCP 等の検討の状況把握等を実施し、その成果を演習参加者等に提供する。

f) 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供をする。

g) 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開をする。

（ク）「障害対応体制の強化」に関する重要インフラ所管省庁の施策 （重要インフラ所管省庁）

a) 内閣官房が情報疎通機能の確認（セプター訓練）等の機会を提供する場合の協力をする。

b) 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力をする。

c) 分野横断的演習へ参加する。

d) セプター及び重要インフラ事業者等の分野横断的演習への参加を支援する。

e) 分野横断的演習の改善策検討への協力をする。

f) 必要に応じて、分野横断的演習成果を重要インフラ所管省庁の施策へ活用する。

g) 分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力をする。

（ケ）「障害対応体制の強化」に関する事案対処省庁の施策 （事案対処省庁）

重要インフラ事業者等からの要望があった場合、IT 障害対応能力を高めるための支援策を実施する。

【 リスクマネジメント 】

（コ）「リスクマネジメント」に関する内閣官房の施策 （内閣官房）

a) リスクマネジメントの標準的な考え方や定義等の利活用や国際標準等を読み替えた手引書等の提示による関係主体間の共通認識を醸成する。

b) 本施策における調査・分析による重要インフラ事業者等におけるリスクマネジメントを支援する。

c) 本施策における調査・分析の結果を安全基準等に反映する基礎資料として提供する。

d) セプターカウンシル及び分野横断的演習等を通じて重要インフラ事業者等のリスクコ

ミュニケーション及び協議を支援する。

(サ)「リスクマネジメント」に関する重要インフラ所管省庁の施策 (重要インフラ所管省庁)

a) リスクマネジメントに関する調査・分析を必要とする対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供する。

b) リスクマネジメントに関する調査・分析を重要インフラ所管省庁の施策へ活用する。

c) 重要インフラ事業者等のリスクコミュニケーション及び協議を支援する。

【 防護基盤の強化 】

(シ)「防護基盤の強化」に関する内閣官房の施策 (内閣官房)

a) Web サイトやニュースレターを通じた広報を実施する。

b) 講演等を通じた公聴活動を実施する。

c) 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携を強化する。

d) 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供する。

e) 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行する。

f) 関連規格を整理、可視化する。

g) 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、必要に応じて、手引書等を整備する。

h) 制御系機器・システムの第三者認証制度の拡充を支援する。

(ス)「防護基盤の強化」に関する重要インフラ所管省庁の施策 (重要インフラ所管省庁)

a) 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携を強化する。

b) 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供する。

c) 内閣官房と協力し、関連規格を整理、可視化する。

d) 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備する。

e) 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援する。

【 その他の施策 】

(セ)大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等 (内閣官房及び関係

府省庁）※再掲

内閣官房において、関係府省庁と協力し、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を実施し、当該結果を踏まえた検討を行うこと等により、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について」、「大規模サイバー攻撃事態等への初動対処について」等に基づき官民が連携して的確な対応を行うことができる態勢を整備する。また、上記訓練は 2015 年度以降も継続して実施する。

（ソ）情報通信分野における事業者との官民連携の推進　（総務省）

総務省において、情報セキュリティ上の事案について、ISP 事業者団体の「テレコム・アイザック推進会議」をはじめとした関係団体等と情報共有を推進する。

（タ）個別分野におけるサイバー演習　（総務省及び経済産業省）

a) 総務省において、巧妙化・複雑化するサイバー攻撃に対応するため、情報通信分野の事業者によるサイバー攻撃対応演習の実施を支援し、事業者間連携等を促進する。

b) 経済産業省において、CSSC を通じて、重要インフラの制御系の情報セキュリティ対策のため、今後、実際にサイバー攻撃が発生することを前提としたサイバー演習又はセミナーを実施し、制御システムのセキュリティ評価及びセキュリティ対策に関する知見を蓄積し、我が国の制御システムのセキュリティ対策に繋げる。

（チ）電気通信システムの安全・信頼性確保　（総務省）

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、適宜「情報通信ネットワーク安全・信頼性基準 [11]」等を見直す。

（ツ）重要無線通信妨害対策の強化　（総務省）

a) 総務省において、重要無線通信妨害事案の発生時の対応強化のため、重要無線通信妨害申告受付の夜間・休日の全国一元化を継続して実施するとともに、夜間・休日における迅速な出動体制を強化する。

b) 総務省において、電波利用秩序維持のため、遠隔操作による電波監視施設等の性能向上を図りつつ、同施設のセンサーを更改する。

c) 総務省において、電波監視施設の高度化・高機能化等、昨今の電波利用環境の変化を踏まえ、電波監視技術に関する調査研究を実施する。

（テ）「サイバー情報共有イニシアティブ」の強化　（経済産業省）

[11] 昭和 62 年郵政省告示第 73 号。

経済産業省において、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、２年間の活動成果を踏まえ、より有効な活動に発展させるよう、産業分野と参加メンバーを拡大させるとともに、共有情報の充実等を図るとともに、引き続きセプターとの情報共有等を推進する。

また、同じく IPA で実施している「標的型サイバー攻撃の特別相談窓口」により得られた標的型攻撃の解析情報等と合わせて、「サイバー攻撃解析協議会」等での高度解析に繋げる。

（ト）サイバー攻撃（インシデント）対応調整支援　（経済産業省）

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。

（ナ）重要インフラで利用される情報システムのセキュリティ・信頼性向上のための支援体制の整備　（経済産業省）

a)　経済産業省において、重要インフラ事業者の情報処理システム等の信頼性・安全性向上のための自発的な取組を支援するため、IPA を通じ、障害事例集の整備・共有や、自発的に提供のあった情報のマクロ的な定量分析・解析、蓄積された情報のセプター等への提供を行う。

b)　経済産業省において、CSSC を通じ、必要に応じ現在策定中の制御システムのセキュリティに係る国際標準について、我が国としての要求事項等について寄書を行う。また、制御システムのセキュリティに係る評価・認証に関して国際的な連携の実施や、既存企画の翻訳等に着手し、国内製品の認証取得を容易化するための検討を行い、結論を得る。

（ニ）重要インフラ事業者に対するソフトウェアや制御システム等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等　（経済産業省）

a)　経済産業省において、IPA 及び JPCERT/CC を通じ、制御システム関係者による計画的な対応及び安全な対策の実施を可能とするよう前年度に行った脆弱性ハンドリング体制の見直し結果を踏まえて、当該体制を運用する。

b)　経済産業省において、重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威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 からセプター又は重要インフラ事業者その他の国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織等に提供する。

c)　経済産業省において、IPA、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の利活用し易い形式での発信を進める。

（ヌ）制御システムに関するインシデントや脆弱性への対応のための連携体制の構築　（経済産業省）

経済産業省において、2012 年７月に起ち上げた JPCERT/CC の制御システムセキュリティ対策グループ（ICSR）を通じ、制御システム関連団体とともに、制御システムにおけるセキュ

リティ対策の推進に資する情報の収集、共有、発信を推進することにより、制御システムに関するインシデントや脆弱性等の脅威への対応の円滑化を図る。

(ネ) 制御システムにおける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確立支援 （経済産業省）

経済産業省において、IPA の推進する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について、2014 年度の確立に向けて、JIPDEC 等関係組織に対して支援を行う。

(ノ) 制御機器等の評価・認証スキームの確立支援 （経済産業省）

経済産業省において、CSSC の推進する制御機器等の評価・認証について、2015 年度の評価・認証機関の確立に向けて、CSSC の取組を支援する。

(ハ) 制御システムセキュリティの国際標準に基づく評価・認証機関設立 （経済産業省）

経済産業省において、日本国内で制御システム等のセキュリティ評価・認証が行えるよう、パイロット認証等の実施を経て体制を確立し、CSSC を中心とした制御システムのセキュリティに関する評価・認証機関の設立を目指す。

(ヒ) 制御システムセキュリティ評価・認証の国際相互承認 （経済産業省）

経済産業省において、CSSC の制御セキュリティ検証施設を利用して研究開発成果の展開を図り、制御システムセキュリティに係る国際標準化の推進とそれをベースにした国際的な相互承認の対象制度の拡大を推進する。

(フ) 制御システムセキュリティ評価・認証の利活用に向けた検討 （経済産業省）

経済産業省において、CSSC による制御システムのセキュリティに関する評価・認証を受けたシステムの導入を推進するための制度整備を進める。

(ヘ) ソフトウェア、情報システムの信頼性向上 （経済産業省）

経済産業省において、重要インフラ分野の情報システムに係るソフトウェア障害情報の収集・分析及び対策や利用者視点でのソフトウェア信頼性の見える化の促進を図る。

(ホ) 社会的に重要な情報システムについての情報セキュリティ強化 （経済産業省）

経済産業省において、重要インフラ分野や制御システム等の社会的に重要な情報システムについて、関係省庁等の求めに応じて、IPA を通じ、情報セキュリティ強化のための調査、協力を行う。

（マ）我が国の重大なセキュリティ事案に対する対応支援 （経済産業省）

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、被害状況を把握し、再発防止に係る対処方針の策定支援を行う。

③ 企業・研究機関等における対策

【 中小企業等における対応強化 】

(ア) 中小企業における情報セキュリティ対策の推進 （経済産業省）

a) 経済産業省において、IPA を通じ、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指導者育成セミナー」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を図るとともに、IPA 等の作成する啓発資料・ツール等の利用を促進する。

b) 経済産業省において、IPA を通じ、情報セキュリティ対策の推進が困難と感じている中小企業における情報セキュリティ対策コストの負担の適正化及び対策の推進を目的として、IPA を通じ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促進する。

(イ) 中小企業における情報セキュリティ対策の底上げ （総務省及び経済産業省）

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。

(ウ) 中小企業・小規模事業者の IT 活用における情報セキュリティの確保 （経済産業省）

中小企業・小規模事業者の新ビジネス創造促進のための IT 活用に対し、IPA において、情報セキュリティ確保等の観点から必要な支援を行う。

(エ) 個人情報漏えい等防止のための対策 （経済産業省）

経済産業省において、標的型攻撃の顕在化を踏まえ、サイバー攻撃等による個人情報漏えい等を防ぐため、必要かつ適切な技術的対策を、個人情報の保護に関する法律[12]（以下「個人情報保護法」という。）のガイドラインに盛り込む。また、これを踏まえつつ、サイバー攻撃等による個人情報漏えい等を防ぐための対策について、個人情報取扱事業者を対象に普及啓発を行う。

(オ) 技術・営業秘密保護に関する官民の情報共有 （経済産業省）

経済産業省において、日本における技術・営業秘密保護のための取組を促進するために、営業秘密保護に関する情報共有・検討などを可能とするための官民連携を推進する。

【 事業等のリスクの開示 】

[12] 平成 15 年法律第 57 号。

(カ) 上場企業における事業等のリスクとしての開示の検討 （金融庁）

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。

(キ) セキュリティエコノミクスに関する対応 （経済産業省）

経済産業省において、企業などの組織にとって最適な情報セキュリティ対策への投資や対策のレベルを評価する仕組みについて、IPA を通じ、経済学などの社会科学の知見を導入した検討を実施する。

【 情報セキュリティガバナンスの確立 】

(ク) 情報セキュリティガバナンス確立の促進 （経済産業省）

経済産業省において、企業の情報セキュリティに係る負担を軽減し、また海外の動向を勘案しつつ、企業における新たな情報セキュリティガバナンスの確立を図るため、情報セキュリティガバナンスの普及啓発や導入支援を進める「情報セキュリティガバナンス協議会」において、情報リスクの管理に関する参加企業内での知見の共有を図る。

(ケ) 企業における情報セキュリティ対策の支援 （経済産業省）

a) 経済産業省において、「2014 年情報処理実態調査」により、企業における情報セキュリティ監査制度の活用・企業における情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況、取引（委託、外注を含む）相手における情報セキュリティ対策実施状況の確認状況、Common Criteria（ISO/IEC15408）認証取得製品の導入状況について調査する。

b) 経済産業省において、国際的な取引等において情報セキュリティ上の信頼性を求められるようになることから、企業における情報セキュリティ監査制度の更なる普及に向けた各種対応を行う。

c) 経済産業省において、企業における適切な情報管理・情報漏えい防止対策を促進し、情報を預ける国民の権利利益の保護に資するため、情報セキュリティ報告書モデルの普及を図る。

(コ)「情報システム・モデル取引・契約書」の活用・普及 （経済産業省）

経済産業省において、情報システムの信頼性向上の観点から、ユーザー・ベンダ間の取引の可視化・役割分担の明確化を進めるため経済産業省が公表した、「情報システム・モデル取引・契約書（第一版）[13]」、「情報システム・モデル取引・契約書（追補版）[14]」、「e ラーニン

[13] 2007 年経済産業省公表。
[14] 2008 年経済産業省公表。

グで学ぶモデル取引・契約書[15]」及び「情報システム・ソフトウェア取引トラブル事例集[16]」について、ユーザー・ベンダ双方の関係業界団体と連携して普及活動を推進する。

(サ) 企業における電子署名利活用の普及促進 （総務省、法務省及び経済産業省）

総務省、法務省及び経済産業省において、セミナーの開催等をはじめ、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。

(シ) 情報システム調達時等における情報セキュリティの確保の支援 （経済産業省）

a) 経済産業省において、JISEC の運用を推進するとともに、情報システム調達時の同制度の利用拡充を図る。

b) 経済産業省において、「暗号モジュール試験及び認証制度」（JCMVP）及び「暗号アルゴリズム確認制度」の運用を推進する。また、JCMVP について、IPA を通じ、試験等に関する人材の育成を図るとともに、NIST との覚書に基づく JCMVP との共同認証制度の運営に着手する。

c) 経済産業省において、IPA を通じ、CCRA における複合機に関するコラボラティブ・プロテクション・プロファイル（cPP）の整備を行う。

(ス) CISO 等の設置促進 （経済産業省）

経済産業省において、情報セキュリティを推進する観点から、CISO の設置の普及等に努める。

(セ) 組織の緊急対応チームの普及、連携体制の強化 （経済産業省）

経済産業省において、JPCERT/CC を通じ、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。

(ソ) 企業の運営するウェブサイトの安全性向上 （経済産業省）

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「ウェブサイト攻撃の検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。

(タ) 内部の不正行為によるセキュリティインシデント防止の検討 （経済産業省）

[15] 2009 年経済産業省公表。
[16] 2010 年経済産業省公表。

経済産業省において、内部者の不正による情報セキュリティインシデントを防止するための方策に関するガイドラインの普及浸透を図る。

(チ) 経営層向けセミナーの開催等 （内閣官房、総務省及び経済産業省）

内閣官房、総務省及び経済産業省において、企業等の経営層、人事担当、採用担当等を対象としたセミナー等の開催や啓発資料の作成を推進するとともに、経済団体等が主催する会議も活用するなど、あらゆる機会を捉えて普及啓発を行う。また、「情報セキュリティガバナンス協議会」の活動を支援する。

(ツ) 実務者層のリーダー層に対する組織内部におけるコミュニケーション能力の強化 （内閣官房、総務省、経済産業省）

実務者層のリーダー層を対象に、経営戦略の視点も理解しつつ組織内の考え方を変革していけるような経営戦略と情報通信技術の利活用、情報セキュリティと事業リスクとの関係などを分析し、伝えていくコミュニケーション能力などの向上を図るためのセミナー等の実施の検討を行う。

(テ) 情報セキュリティ対策に資する各種ツール・分析等の提供 （経済産業省）

経済産業省において、IPA を通じ、情報セキュリティ対策ベンチマークを提供する。

【 教育機関における取組の強化 】

(ト) 地方公共団体の教育関係部門における情報セキュリティに関する取組の推進 （文部科学省）

文部科学省において、教育関係部門での情報セキュリティを確保するため、情報セキュリティの取組に関する普及・啓発を推進するとともに、情報セキュリティを含む情報通信技術の活用指導力の向上を目的とした取組が地方公共団体等において進められるよう、各地域で情報教育を推進する中核的な役割を担う指導主事等を対象とした研修を行う。

(ナ) 大学に対する情報セキュリティに関する最新情報の提供 （内閣官房、総務省、文部科学省及び経済産業省）

内閣官房、総務省、文部科学省及び経済産業省において、大学における情報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。

【 その他 】

(ニ) 個人情報保護法の見直し （内閣官房、消費者庁及び関係府省庁）

内閣官房、消費者庁及び関係府省庁において、個人情報保護法について、IT 総合戦略本部

において決定された「パーソナルデータの利活用に関する制度見直し方針[17]」を踏まえ、同法改正に係る検討を行う。

[17] 2013年12月20日IT総合戦略本部決定。

④ サイバー空間の衛生

【 普及啓発 】

(ア) 新たな情報セキュリティ普及啓発プログラムの策定 （内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、「情報セキュリティ普及・啓発プログラム[18]」の見直しを行い、2014 年度以降の具体的な取組について「新たな情報セキュリティ普及・啓発プログラム」（仮称）を策定し、公表する。

(イ) 各府省庁と連携した普及啓発活動の推進 （内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、文部科学省、経済産業省、防衛省及び関係省庁）

内閣官房において、内閣府、警察庁、消費者庁、総務省、外務省、文部科学省、経済産業省、防衛省及び関係省庁と協力し、相互の連携強化を図るため、関係府省庁との連絡会等を定期的に開催する。

(ウ)「サイバーセキュリティの日」の取組の推進 （内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、文部科学省、経済産業省、防衛省及び関係省庁）

内閣官房、内閣府、警察庁、消費者庁、総務省、外務省、文部科学省、経済産業省、防衛省及び関係省庁において、一般利用者等の認識の更なる醸成を図るため、「サイバーセキュリティの日」の取組を推進する。

(エ) ソフトウェア教育との連携 （内閣官房及び文部科学省）

内閣官房において、文部科学省と協力し、情報セキュリティの基礎となるソフトウェア教育等と連携した普及啓発を進める。

(オ) 表彰等の充実 （総務省及び経済産業省）

a) 総務省及び経済産業省において、情報セキュリティ確保の観点から、多大な貢献を果たした個人・企業等を表彰する。

b) 経済産業省において、「未踏 IT 人材発掘・育成事業」を実施する。

(カ)「情報セキュリティ月間[19]」の充実 （内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、これまでの「情報セキュリティ月間」の実施結果等を踏まえ、国民に対するより一層効果的な情報発信の方法や官民連携の強化等について検討を行い、「情報セキュリティ月間」における取組の充実と更なる周知を図る。

---

[18] 2011 年７月情報セキュリティ政策会議決定。
[19] 毎年２月。

(キ) 国際連携を活用した国内外における普及・啓発活動の実施 （内閣官房及び関係府省庁）

内閣官房及び関係府省庁において、ASEAN、欧米を始めとする諸国と国際連携を活用した行事や情報セキュリティ対策に関する情報提供等を行う「情報セキュリティ国際キャンペーン [20]」を実施し、国際連携の一層の推進と、国内における情報セキュリティ対策の更なる普及・啓発を図る。

(ク)「新たな情報セキュリティ普及・啓発プログラム」（仮称）の推進 （内閣官房及び関係府省庁）

a) 内閣官房において、各府省庁と協力し、「新たな情報セキュリティ普及・啓発プログラム」（仮称）に基づき、同プログラムに掲げられた施策を着実に推進する。

b) 内閣官房において、各府省庁と協力し、国民一人ひとりの情報セキュリティについての関心を高めるため、自ら実施している対策がどのフェーズにあるのかを客観的に認識するためのツールである自己診断チェックリストの活用を進める。

c) 内閣官房において、各府省庁と協力し、高齢者層に対していたずらに不安感を煽ることのないように配慮しつつ、平易な言葉で情報セキュリティ対策を分かりやすく伝えるため高齢者向け資料の活用を進める。

d) 内閣官房において、各府省庁と協力し、企業の経営層が情報セキュリティに関する認識を高め、情報セキュリティに関するリスク判断を適切に行えるようにするための情報提供を行う。

e) 内閣官房において、各府省庁や事業者等と連携し、保護者や学校の教職員、児童生徒を対象とした啓発活動や、学習・参加型のシンポジウム等を引き続き推進する。

(ケ) 各種メディア等を通じた普及・啓発の推進 （内閣官房、警察庁、総務省、文部科学省及び経済産業省）

a) 内閣官房において、各府省庁と協力し、国民の情報セキュリティ意識の向上を図るため、急速に高度化・複雑化している情報セキュリティ上の脅威に関する情勢等を踏まえ、「国民を守る情報セキュリティサイト」、「@police」、「国民のための情報セキュリティサイト」、「インターネット安全教室」、「フィッシング対策協議会」、「フィッシング対策推進連絡会」、「情報セキュリティ安心相談窓口」、「ここからセキュリティ！」等を通じ、国民一人一人に対する適切な情報提供を実施する。これらの取組においては、IT 初心者の層だけでなく、情報セキュリティ無関心層に対する働き掛けも重視することとする。

b) 警察庁において、情報セキュリティに関する意識・知識の向上を図るため、教育機関関係者、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、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 等の最新の情報通信技術を悪用した犯罪等の身近な脅威等を交えた講演等の全国的な実施を推進する。

c) 総務省と文部科学省が協力し、保護者、教職員及び児童生徒を対象に、子どもたちのインターネットの安心・安全な利用に向けた啓発のための講座（「e-ネットキャラバン」）を、通信関係団体等と連携しながら全国規模で実施する。

---

[20] 2012 年より毎年 10 月に実施。

d) 総務省において、各府省庁と協力し、スマートフォン等が急速に普及していることを踏まえ、利用者に対して、スマートフォン等の情報セキュリティ対策について引き続き総合的な普及・啓発を推進する。

e) 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。

f) 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。

g) 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、情報セキュリティに関するコンクール、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。

h) 経済産業省において、IPA、JPCERT/CC における統合的な脆弱性対策情報の提供環境を整備し、開発者、運用者及びエンドユーザーに対して、脆弱性対策の普及啓発を推進する。

i) 経済産業省において、急速に変化しつつある脅威を的確に把握し、ウイルスや不正アクセス等の情報を積極的に収集・分析し、IPA を通じ広く国民一般に対し、傾向や対策等情報提供を行うとともに、「情報セキュリティ安心相談窓口」の運用により得た情報を踏まえ、コンピュータ利用者への注意喚起等の対策に反映する。

(コ) 情報セキュリティに関する事故事例等に関する普及啓発の推進　（内閣官房、経済産業省及び関係府省庁）

内閣官房及び経済産業省において、各府省庁と協力し、IPA 等に集約される情報セキュリティに関する事故事例等について、プライバシー保護など情報提供者等に配慮した上で収集し、主に一般国民を対象に普及啓発を進める。

(サ) 無線 LAN の情報セキュリティ確保の推進　（総務省）

総務省において、一般及び企業による利用が拡大する一方、情報窃取等の情報セキュリティ上の課題が指摘されている無線 LAN について、作成したテキストを活用し、引き続き適切な無線 LAN の情報セキュリティ対策の普及・啓発に努める。

(シ) 電波利用秩序維持のための周知啓発活動の強化　（総務省）

総務省において、毎年６月の電波利用環境保護周知啓発強化期間において、新聞、電車の中吊り広告、ホームページ等の各種メディアにより周知啓発を実施する。

(ス) 情報漏えい対策への取組　（経済産業省）

a) 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。

b) 経済産業省において、情報漏えいの新たな手法や手口の情報収集に努め、一般国民に対し、対策情報等、必要な情報提供を行う。

【 インシデントの認知・解析機能の向上 】

(セ) サイバー攻撃高度解析機能の整備 （総務省及び経済産業省）

総務省及び経済産業省並びに NICT、IPA、テレコム・アイザック推進会議及び JPCERT/CC の４団体が参加する「サイバー攻撃解析協議会」において、攻撃手法がますます複合化・複雑化するサイバー攻撃に対応するため、各団体が自らの活動やプロジェクト等により得られたサイバー攻撃関連情報を結集し、高度な解析を行う。その解析結果については、各機関の活動や外部への情報提供を通じて、サイバー攻撃への対処に活用する。また、攻撃手法がますます複合化・複雑化するサイバー攻撃に対応するため、官民関係者がそれぞれ把握できる情報を結集し、それらに対して高度解析を加える仕組みの運用を進める。

(ソ) サイバー攻撃（インシデント）対応調整支援 （経済産業省）※再掲

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。

(タ) サイバー攻撃の予兆の早期把握と情報収集・分析の強化 （警察庁及び法務省）

警察庁及び法務省において、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、オープンソースの情報を幅広く収集するなど、攻撃主体・方法等に関する情報収集・分析を強化する。

(チ) サイバー攻撃事案の実態解明に係る情報収集・分析等 （警察庁）

a) 警察庁において、違法行為に対する捜査等を推進するため、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。

b) 警察庁において、サイバー攻撃事案の実態解明に資するよう、インターネット観測技術に関する調査研究を行う。

(ツ) 新しい脅威・攻撃の分析・共有 （経済産業省）

経済産業省において、IPA の運営する「脅威と対策研究会」を通じ、情報セキュリティに関する新しい脅威・攻撃を分析するとともに、分析結果等の利用者に必要な情報を迅速に提供する。

(テ) コンピュータセキュリティ早期警戒体制の強化 （経済産業省）

a) 経済産業省において、サイバー攻撃によるインシデント（制御システムに係るもの及び巧妙かつ執拗に行われる標的型攻撃に係るものを含む。）、脆弱性等に関する迅速な情報共有、円滑な対応を確保するため、IPA や JPCERT/CC 等による対応・対策を強化する。具体的には、脆弱性情報を IPA で受付、JPCERT/CC が公開に向けた調整を行うほか、近時のコンピュータウイルス等の攻撃手法の巧妙化に対応するため、インシデント対応の調整支援を行う JPCERT/CC 等の組織において、攻撃手法の分析・解析能力の一層の高度化、専門家間での解析手法やインシデント事例等に関する情報共有・連携を推進する。

b) 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。

c) 経済産業省において、2012 年度に整備した制御システムに係るインシデントに特化した対応調整支援体制や、巧妙かつ執拗に行われる標的型攻撃に係る対応手法について、JPCERT/CC における効果的な運用を進めつつ、報告受付制度や対処手法の普及を図る。

d) 経済産業省において、フィッシング対策協議会及び JPCERT/CC を通じた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について、不正アクセス禁止法[21]も踏まえ実施する。

(ト) 注意喚起等による情報セキュリティリスクの低減 （経済産業省）

経済産業省において、IPA を通じ、最新の脆弱性情報やインシデント情報を収集、分析し、注意喚起による危険回避や対策の徹底を図り、情報セキュリティリスクの低減を促進する。

(ナ) サイバー攻撃事前防止・早期対策に向けた取組の推進 （総務省）

a) 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ネットワークを国際的に構築し、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。

b) 総務省において、米国とは、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、サイバー攻撃に関するデータを共有し、研究開発の分野での協力関係を加速化していくべきであるということで一致したことを踏まえ、サイバー攻撃の予兆を検知し迅速に対応することを可能とする技術の研究開発等を効果的に実施するため、データの共有を開始しているところであり、引き続き、米国との情報共有を強化する。

c) 総務省において、EU とは、引き続き、ネットワーク上の攻撃の軽減のための共同研究の実施等の課題について議論を進める。

d) 総務省において、ASEAN 諸国との連携プロジェクトである JASPER による連携を推進する。

---

[21] 不正アクセス行為の禁止等に関する法律。平成 11 年法律第 128 号。

(ニ) 高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築 （総務省）

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、ネットワーク型のボットウイルスに感染したユーザーを検知し、マルウェアの除去を当該ユーザーに促す取組を継続するほか、マルウェアを配布する等の悪性サイトにユーザーが気付かない間に誘導されるようなサイトも注意喚起等の対象に含め、ISP 等との連携による Web 感染型マルウェア対策の高度化を図る。

また、得られたサイバー攻撃関連情報については、必要に応じて、サイバー攻撃解析協議会や学会等に対して提供し、連携を図る。

(ヌ) 情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用の在り方の検討 （総務省）

総務省において、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」のとりまとめを踏まえ、ISP など電気通信事業者等において、関係ガイドラインの改定など具体的な取組が行われることを支援するとともに、今後も必要に応じ、サイバー攻撃への適正な対処の在り方について検討を行う。

【 ソフトウェアの脆弱性への対応 】

(ネ) 脆弱性に関する情報収集・提供 （経済産業省）

経済産業省において、従来の届出の受付等に基づく脆弱性関連情報の調整・提供のみならず、自ら能動的にサイバー攻撃や脆弱性の検出を行い、調整・提供につなげるための取組を行う。

(ノ) 脆弱性関連情報届出受付制度の運営及び脆弱性関連情報の提供 （経済産業省）

経済産業省において、IPA と JPCERT/CC 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。

(ハ) ソフトウェア等の脆弱性に係るマネジメントの支援等 （経済産業省）

a) 経済産業省において、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に関する JPCERT/CC の活動を強化する。

b) 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。

(ヒ) ソフトウェアや情報システムの安全な利用の推進及び脆弱性の発生を縮減するための対策の推進 （経済産業省）

a) 経済産業省において、経済産業省告示[22]に基づき、脆弱性関連情報の届出受付を行い、定期的に受付状況を公表するとともに、関係者との連携を図りつつ、脆弱性関連情報をウェブサイト運営者、ソフトウェア製品開発者に提供し、脆弱性対策を促進する。

b) 経済産業省において、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 JPCERT/CC 等の取組を継続する。

c) 経済産業省において、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。

d) 経済産業省において、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」をセットにして IPA を通じて普及啓発を図る。

e) 経済産業省において、自動車に含まれるソフトウェアを活用したサービスの増加や、スマートフォン等の普及による自動車と外部ネットワークの連携強化を受け、IPA を通じて自動車の情報セキュリティ対策の普及を図る。

f) 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。

(フ) 脆弱性ハンドリングの国際調整 （経済産業省）

経済産業省において、JPCERT/CC を通じ、FIRST における、全世界で公開される全ての脆弱性情報を言語を問わず集約し、識別できるようにする仕組み構築するための取組に引き続き参加し、協力する。

(ヘ) 組込み機器の脆弱性対策の推進 （経済産業省）

経済産業省において、IPA を通じ、我が国の競争力の源泉となる組込み機器の脆弱性に関する調査と対策の提示等を行う。

(ホ) 情報システム等の安全性・信頼性等に関する利用者への品質説明力の強化 （経済産業省）

経済産業省において、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・

[22] 「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。

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。

【 その他 】

(マ) スパムメール対策の強化 （消費者庁及び総務省）

a) 消費者庁及び総務省において、巧妙化・悪質化が進展し全体として増加が続くスパムメールに対応するため、特定電子メール法及び特定商取引法の着実な執行等所要の措置を講じる。

b) 総務省において、国内の主要なインターネット接続サービス事業者や携帯電話事業者等の業界団体と連携して、スパムメール送信の防止に効果のある技術である 25 番ポートブロックや送信ドメイン認証技術（SPF、DKIM 等）等の導入を促進する。

c) 総務省において、我が国に着信するスパムメールの大部分を占める海外から発信されるスパムメールに対応するため、スパムメール対策を行う外国執行当局との連携を強化するとともに、民間における国際的なスパムメール対策の連携を推進する。

d) 総務省において、その他、違法なスパムメールに関する情報を当該スパムメールの送信等に利用されたインターネット接続サービス事業者に通知し利用停止等の措置を促進する「迷惑メール追放支援プロジェクト」を実施する。

(ミ) 暗号・認証技術等を用いた通信プロトコルの利用による安全な通信環境の実現 （総務省）

総務省において、NICT を通じ、安全な通信環境の実現に向け、暗号・認証技術等を利用した通信プロトコルの安全性に関する評価を実施するとともに、評価結果の情報を集約してプロトコルの脆弱性情報の提供を行う。

(ム) IPv6 ネットワークのための情報セキュリティ検証環境の構築 （総務省）

総務省において、NICT を通じ、IPv6 ネットワークの情報セキュリティの確保に向け、IPv6 への移行に伴う脅威や脆弱性等の具体的なセキュリティ課題を抽出し、これまで構築してきた検証環境を用いてそれらの重要度を評価した上で、必要な情報セキュリティ対策の研究開発を行う。

⑤ サイバー空間の犯罪対策

【 サイバー攻撃対策等の強化 】

(ア) サイバー攻撃対策に係る態勢等の強化 （警察庁）

サイバー犯罪・サイバー攻撃手法の高度化等に対応するため、以下に掲げる施策を実施して、警察におけるサイバーセキュリティ対策に係る態勢等の強化を推進する。

a) 警察庁にサイバーセキュリティ対策を担当する長官官房審議官及び長官官房参事官を設置して司令塔機能を強化し、統一的な戦略の下で、サイバー空間の脅威への警察全体の対処能力を強化する。

b) 警察大学校に「サイバーセキュリティ研究・研修センター」を設置し、サイバー犯罪・サイバー攻撃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。

c) 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。）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、サイバー犯罪の取締りを行うための資機材の整備の推進、全国協働捜査方式による取締りの推進等、サイバー犯罪への対処態勢を強化する。

d) サイバー攻撃の予兆を把握するため、サイバー空間上の情報を収集する機能を持つ資機材を整備するとともに、「サイバー攻撃特別捜査隊」を中心として、全国の都道府県警察におい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。

e) 警察庁に設置した「サイバー攻撃分析センター」にサイバー攻撃に関する捜査情報、不正プログラムの解析情報等を集約し、その実態を解明するために必要な分析機能を持つ資機材を整備するなど、その態勢を拡充し、情報の収集・分析や広域捜査・国際捜査を推進するための体制を強化する。

f) 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向上等を通じて、サイバー攻撃対策に係る体制等を強化する。

g) サイバー攻撃対策要員の事案対処能力・技術力の維持・向上のため、民間の知見を活用した研修を実施するとともに、サイバー空間の脅威に関する知見を有するセキュリティ関連事業者に対し、サイバー攻撃に関する情報について調査を委託し、情報の提供を受ける。

h) 警察庁において、重要インフラ事業者等からの要望に基づく IT 障害対応能力を高めるための支援を実施するため、重要インフラの基幹システムに対するサイバー攻撃発生時における被害の未然防止・拡大防止、障害発生の原因の究明等の方策について調査を行い、サイバーテロ対策の強化につなげる。

(イ) 日本版 NCFTA の創設に向けた検討 （警察庁）

2013 年度総合セキュリティ対策会議での議論を踏まえ、日本版 NCFTA の創設に向け、実務的・具体的な検討を推進する。

(ウ) サイバー空間の安全と秩序を維持するための民間との連携強化 （警察庁）

サイバー空間の安全と秩序を維持するため、各都道府県警察と関係事業者等から成る各種協議会等を通じ、官民連携した取組を推進する。

(エ) 犯罪に強い IT 社会構築のための官民連携に向けた取組の推進 （警察庁）

有識者、関連事業者等で構成する総合セキュリティ対策会議を開催し、サイバー空間の脅威に対処するための産学官連携の在り方について検討し、結論を得る。

(オ) サイバー犯罪の被害防止対策の推進 （警察庁）

インターネット利用者の各種トラブルに応じた基本的な対応策やサイバー犯罪の手口やその対応策を警察庁ウェブサイトに掲載するなどの広報啓発を実施する。

(カ) 不正アクセス禁止法の適正な運用を始めとした不正アクセス防止対策の推進 （警察庁、総務省及び経済産業省）

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、情報セキュリティ関連事業者団体に対する不正アクセス行為の具体的手口に関する最新の情報の提供や、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。

(キ) フィッシング対策協議会 （経済産業省）

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) 重要インフラに対するサイバーテロ対策に係る官民の連携強化 （警察庁）

都道府県警察において、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ことにより、昨今の我が国政府機関等に対するサイバー攻撃事案の発生等を踏まえた、サイバーテロに対する危機意識の醸成を図るとともに、事案発生を想定した共同訓練の実施やサイバーテロ対策協議会を通じた事業者間の情報共有により、重要インフラ事業者等の意向を尊重し、サイバーテロ発生時における緊急対処能力の向上に資する取組を行う。

(ケ) サイバーインテリジェンス対策に係る官民の連携強化 （警察庁）

サイバー攻撃の標的となるおそれのある事業者等との情報共有体制を強化し、サイバーインテリジェンス対策に資する取組を行う。

【 事後追跡可能性の確保 】

(コ) ログの保存の在り方の検討 （警察庁及び総務省）

警察庁及び総務省において、相互に連携しつつ、サイバー犯罪に対する事後追跡可能性を確保するため、可能な範囲で速やかに一定の結論を得るよう、関係事業者における通信履歴等に関するログの保存の在り方について検討する。

特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログ保存期間、一般利用者としての国民の多様な意見等を勘案した上で、サイバー犯罪における捜査への利用の在り方についての検討を行う。

(サ) デジタルフォレンジックに係る取組の推進 （警察庁）

a) 多様化・複雑化するサイバー犯罪に適切に対処するため、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、資機材の増強のほか、関係会合への参加や技術協力を通じた関係機関及び民間との協力等、デジタルフォレンジックに係る体制等の強化を推進する。

b) 高度情報技術解析センターを中心として、不正プログラムの解析のための体制等を強化する。

c) デジタルフォレンジックを取り巻く課題とその対応方策に関する調査研究を行う。

【 人材育成等による体制強化 】

(シ) サイバー犯罪対策のための人材育成の強化 （法務省）

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。

(ス) サイバー防犯ボランティア育成の推進 （警察庁）

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及び育成や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。

【 その他 】

(セ) スマートフォンの安全利用のための環境整備 （警察庁）

スマートフォン利用者等を狙ったサイバー犯罪等の減少に向け、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。

（ソ）スマートフォン利用者等を狙ったサイバー犯罪への対処 （警察庁）

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。

⑥ サイバー空間の防衛

【 自衛隊等の態勢の強化 】

(ア) サイバー情報収集装置の整備 （防衛省）

サイバー空間における脅威が複雑化・巧妙化している状況の中で、サイバー攻撃の兆候を早期に察知し、未然防止に資する情報収集装置を整備する。

(イ) 次期サイバー防護分析装置のシステム設計等 （防衛省）

サイバー防護分析装置の換装に向けて、防衛省に対するサイバー攻撃への対処を統合的に実施するためのシステム設計等を実施する。

(ウ) サイバー防護分析装置の機能強化 （防衛省）

防衛省において、サイバー攻撃等に関する技術は日々進歩していることを踏まえ、サイバー防護分析装置の情報収集機能や分析機能、演習機能の強化等、技術の進化に対応した機能向上等を行う。

(エ) 防衛情報通信基盤（DII）の整備 （防衛省）

防衛省・自衛隊の各部隊等間における確実な指揮命令の伝達と迅速な情報共有を行うために不可欠な防衛情報通信基盤（DII）のクローズ系に最新技術を適用し、セキュリティの向上を図りつつ、情報共有機能を強化する。

(オ) ネットワークサイバー攻撃対処技術の研究 （防衛省）

サイバー攻撃の生起時に、ネットワーク内において迅速に経路変更等を行うことにより、重要通信の経路を確保し、被害拡大を防止するための研究を実施する。

(カ) サイバー演習環境構築技術に関する研究 （防衛省）

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。

(キ) ネットワーク監視態勢の強化 （防衛省）

防衛省において、防衛情報通信基盤（DII）について、サイバー攻撃等に関する状況把握能力を向上させるとともに、サイバー攻撃等発生時における被害局限化、早期復旧等の対処能力を強化するため、ネットワーク監視器材を整備する。

(ク) 陸自電算機防護システムの整備等 （防衛省）

防衛省において、陸上自衛隊の情報システムを対象とした陸自電算機防護システム等、各自衛隊の情報システムを監視、防護するための機材を整備する。

(ケ) 国外におけるサイバー攻撃関連情報に関する情報収集・分析機能強化 （防衛省）

防衛省において、2014 年度以降、情報本部等による国外におけるサイバー攻撃関連情報の収集・分析体制を強化・向上させる。

(コ) 情報保証に係る最新技術動向等の調査研究 （防衛省）

防衛省において、情報システムの情報保証を確保するため、サイバー攻撃及びサイバー攻撃対処に係る最新技術動向等を調査するとともに、有効な対処態勢等について調査研究を実施する。

(サ) 人材育成及び外国との連携強化 （防衛省）

防衛省において、サイバー攻撃等対処に向けた人材育成の取組として、国内外の大学院等への留学等を行う。また、米国等との連携を強化するため各種会議等への参加を行う。

(シ) 民間企業等との連携強化 （防衛省）

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の実施及び防衛省と防衛産業によるサイバー攻撃対処に係る情報を、情報の保全性を確保しつつ、迅速かつ効率的・効果的に共有するための新たな官民情報共有システムを導入する。

【 国家レベルのサイバー攻撃への対応の強化 】

(ス) 国家レベルのサイバー攻撃への対応の強化 （内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係府省庁）

内閣官房において、警察庁、総務省、外務省、経済産業省及び防衛省等の関係府省庁と協力し、外国政府等の関与が疑われる国家レベルのサイバー攻撃への対応体制の整備等を行うため、サイバー攻撃に関するインシデントの認知、インシデント情報等の収集・共有や高度な解析及びわが国に甚大な被害が生じるサイバー攻撃が発生した場合の対処の在り方等について、個別具体的な国際法の適用も整理しつつ、NISC の機能強化等に関する方針を策定し、同方針に基づき、平時及び非常時における警察、防衛省・自衛隊等の政府機関やサイバー空間関連事業者など関係機関の役割の整理・明確化を行う。

２「活力ある」サイバー空間の構築

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

2014 年度においては、「情報セキュリティ研究開発戦略」及び「情報セキュリティ人材育成プログラム」の改定を受けて、最新の脅威に対応したより高度かつ実践的な研究開発の推進、セキュリティ関連人材の量的拡大と質的向上に資する諸施策を具体化し、サイバーセキュリティ関連産業の育成、人材の「需要」と「供給」の好循環の形成を促す。

① 産業活性化

(ア) M2M における情報セキュリティの確保に関する検証等の推進 （総務省）

総務省において、M2M について、情報の機密性や完全性等が失われた場合、社会的混乱を招くばかりでなく、情報通信技術基盤に対する信頼が損なわれる可能性があることから、M2M の認証など情報セキュリティ確保に関する検証等を実施する。

(イ) スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進（経済産業省）

経済産業省において、BEMS 等の先進的なエネルギー設備導入にあたってのサイバーセキュリティ確保の研究開発を行う。

(ウ) 新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発 （総務省）

総務省において、NICT を通じ、クラウド等の新たな情報流通形態に対応するため、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。

(エ) 省リソースデバイスにおける情報セキュリティ技術の研究開発 （総務省）

総務省において、NICT を通じ、スマートメータセンサー等の省リソースデバイスに実装可能な軽量暗号技術や大規模ノードにおける認証・プライバシー保護技術等の研究開発を行う。

(オ) クラウドサービスレベルのチェックリスト等の普及・促進 （経済産業省）

経済産業省において、クラウドコンピューティング利用時におけるデータ保護及びサービス品質に関する責任主体を明確化するために、サービス提供側に過度の負担とならないよう、クラウド事業者とクラウド利用者の間で、サービス内容・範囲・品質等（例：サービス稼働率、信頼性レベル、データ管理方法、セキュリティレベル等）に関する保証基準の共通認識の形成を促す、クラウドサービスレベルのチェックリスト等を普及・促進する。

(カ) クラウドコンピューティングの国際標準化に向けた取組 （総務省及び経済産業省）

a) 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。

b) 経済産業省において、2011 年に策定した「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」の改訂を行うとともに、クラウドセキュリティガイドライン活用ガイドブックとともに公開する。また、ISO/IEC 27000 シリーズに標準として組み入れるべく日本案を ISO/IEC JTC1/SC27 WG1 に提案をしているが、この標準化を推進する。

(キ) 制御システムセキュリティの国際標準に基づく評価・認証機関設立 （経済産業省）※再掲

経済産業省において、日本国内で制御システム等のセキュリティ評価･認証が行えるよう、パイロット認証等の実施を経て体制を確立し、CSSC を中心とした制御システムのセキュリティに関する評価・認証機関の設立を目指す。

(ク) 制御システムセキュリティ評価・認証の国際相互承認 （経済産業省）※再掲

経済産業省において、CSSC の制御セキュリティ検証施設を利用して研究開発成果の展開を図り、制御システムセキュリティに係る国際標準化の推進とそれをベースにした国際的な相互承認の対象制度の拡大を推進する。

(ケ) 国際的なルールに基づくセキュリティ製品の貿易の推進 （経済産業省）

経済産業省において、日本が強みを持つ複合機や制御システム等の日本製品が貿易において不利な扱いを受けることがないよう、IPA を通じ、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組みに積極的に参画、働きかけを進める。

(コ) 自動車に係る情報セキュリティの確保 （経済産業省）

経済産業省において、携帯端末等の機器との相互接続が拡大する自動車の制御システムに関するセキュリティ上の諸問題について調査し対策等の検討を行い、結論を得る。

(サ) 安全性確保のためのソフトウェア等のリバースエンジニアリングの適法性の明確化（文部科学省）

文部科学省において、文化審議会著作権分科会の報告に基づき、情報セキュリティ目的のリバースエンジニアリングの適法性を明確化するための措置を速やかに講ずる。

② 研究開発

（ア）「情報セキュリティ研究開発戦略[23]」の研究開発の推進 （内閣官房及び関係府省庁）

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

（イ）スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進（経済産業省）※再掲

経済産業省において、BEMS 等の先進的なエネルギー設備導入にあたってのサイバーセキュリティ確保の研究開発を行う。

（ウ）標的型攻撃の対策技術に関する研究開発 （総務省）

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。

（エ）情報セキュリティ強化を含むビッグデータ利活用のための研究開発 （文部科学省）

文部科学省において、ビッグデータ利活用のための研究開発として、データ連携技術等（データの収集、蓄積・構造化、データ処理・分析、処理結果の可視化・検証等の各段階における技術等）の研究開発を実施する中で、情報セキュリティ強化のための取組を実施する。

（オ）新世代ネットワーク基盤技術に関する研究開発 （総務省）

総務省において、2020 年頃の実現を視野に、現在のインターネットの限界を克服し、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。

（カ）量子情報通信ネットワーク技術の研究開発 （総務省）

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からなる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。

（キ）ネットワーク等の安全性・信頼性確保に資する情報セキュリティ技術に関する研究開発（総務省）

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。

---

[23] 2011 年７月８日情報セキュリティ政策会議決定。2014 年６月改訂予定。

(ク) 情報通信構成要素の安全性検証技術の高度化に関する研究開発 （総務省）

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。

(ケ) サイバーセキュリティ研究基盤の構築 （総務省）

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。

(コ) システムにおける適切な情報セキュリティ設定を自動的に導出する技術の研究開発の推進 （総務省）

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。

(サ) セキュアでグリーンなクラウドコンピューティング環境の整備 （経済産業省）

経済産業省において、経営・事業戦略に柔軟に対応できる伸縮自在で高効率・高信頼な情報システムを、企業や官公庁といったビジネスシーンでユーザーが安心・安全に利用できるよう、クラウドコンピューティングに係る省エネ、セキュリティ及び安定した稼働を確保する信頼性向上に関する技術等についての実証を行う。

(シ) スマートフォンにおけるリスクの可視化 （総務省）

総務省において、NICT を通じ、スマートフォンの多様な利用形態に応じたリスク評価結果の可視化を行う技術の研究開発を行う。

(ス) イノベーション創出を支える情報基盤強化のための新技術開発 （文部科学省）

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。

(セ) M2M における情報セキュリティの確保に関する検証等の推進 （総務省）※再掲

総務省において、M2M について、情報の機密性や完全性等が失われた場合、社会的混乱を招くばかりでなく、情報通信技術基盤に対する信頼が損なわれる可能性があることから、M2M の認証など情報セキュリティ確保に関する検証等を実施する。

（ソ）省リソースデバイスにおける情報セキュリティ技術の研究開発 （総務省）※再掲

総務省において、NICT を通じ、スマートメータセンサー等の省リソースデバイスに実装可能な軽量暗号技術や大規模ノードにおける認証・プライバシー保護技術等の研究開発を行う。

（タ）新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発 （総務省）※再掲

総務省において、NICT を通じ、クラウド等の新たな情報流通形態に対応するため、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。

（チ）サイバー攻撃事前防止・早期対策に向けた取組の推進 （総務省）※再掲

a) 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ネットワークを国際的に構築し、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。

b) 総務省において、米国とは、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、サイバー攻撃に関するデータを共有し、研究開発の分野での協力関係を加速化していくべきであるということで一致したことを踏まえ、サイバー攻撃の予兆を検知し迅速に対応することを可能とする技術の研究開発等を効果的に実施するため、データの共有を開始しているところであり、引き続き、米国との情報共有を強化する。

c) 総務省において、EU とは、引き続き、ネットワーク上の攻撃の軽減のための共同研究の実施等の課題について議論を進める。

d) 総務省において、ASEAN 諸国との連携プロジェクトである JASPER による連携を推進する。

（ツ）サイバー攻撃の解析・検知に関する研究開発 （総務省）

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。

（テ）サイバーセキュリティ研究開発拠点の構築 （総務省）

総務省において、NICT を通じ、「サイバー攻撃対策総合研究センター（CYREC）」において、サイバー攻撃のモニタリング（観測）・解析の高度化に向け、官民の英知を集めたオールジャパン体制での研究開発・実証実験を実施する。また、同センターにおいては、産業界との連携を強化するとともに、NICT における高度情報セキュリティ人材の育成を促進する。

（ト）制御システムセキュリティに関する研究開発 （経済産業省）

経済産業省において、CSSC が宮城県多賀城市に構築したテストベッド施設を中核として、制御システムのセキュリティ検証方法及び第三者による評価・認証方法に関する研究開発に

取り組み、日本発の技術的基盤を確立する。

（ナ）産業技術総合研究所（AIST）における研究開発の促進 （経済産業省）

経済産業省において、AIST を通じ、拡散するリスクに対して、国民の情報や権利、社会システム等を保護するための情報セキュリティ技術の確立などに向けた先端技術の開発に取り組む。

③ 人材育成

（ア）「新・情報セキュリティ人材育成プログラム[24]」の推進 （内閣官房）

内閣官房において、「新・情報セキュリティ人材育成プログラム」に基づき施策を推進していく。

（イ）リカレント教育の促進 （文部科学省）

文部科学省において、高等教育機関等における社会人学生受入れを支援する。

（ウ）情報セキュリティに関する教育における産学連携の促進 （文部科学省及び経済産業省）

a) 文部科学省において、産学連携により実践的教育を推進する体制の構築や、インターンシップや PBL（課題解決型学習）の実施を支援する。

b) 経済産業省において、実践的インターンシップモデルに基づく企業等と大学・学生のマッチングに関する情報発信を行う。

c) 文部科学省及び経済産業省において、産業界と教育界が協力して作成された授業や教材のデータベースを拡充するとともに、その利用促進を図る。

（エ）大学等における情報セキュリティに関する教育 （内閣官房、総務省、文部科学省及び経済産業省）

a) 文部科学省において、複数大学や産学連携による高度で実践的な教育活動の支援を行う。

b) 内閣官房、総務省、文部科学省及び経済産業省において、情報セキュリティに関する研究科等の設置に資するよう、情報セキュリティに関する最新の情報を大学等に対し積極的に提供する。

（オ）情報セキュリティに係る競技会・演習等の実施 （総務省及び経済産業省）

a) 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」にて共催してきたセキュリティ・キャンプについて、更なる充実を図るとともに、キャンプ卒業生の社会における採用・活用を促進するなど更なる深化を図る。

b) 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 2014」）について経済産業省にお

[24] 「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）を改訂。

いて普及・広報の支援を行う。

c) 総務省及び経済産業省において、情報セキュリティ人材が、最新の防御モデルに基づくサイバー攻撃への対処方策を体験できるような演習又はセミナーを実施する。

(カ) 横断的キャリアパス・モデルの普及、人材育成計画の策定促進 （経済産業省及び関係府省庁）

経済産業省において、関係府省庁と協力し、IPA が策定した情報セキュリティ人材のキャリアパス・モデルの普及に努めるとともに、企業等における人材育成計画の策定を促進する。

(キ) スキル、資格、教育プログラム等の整理 （経済産業省）

経済産業省において、情報セキュリティ関連業務で求められるスキルと関連する資格、教育プログラムを整理した結果の普及浸透を図るとともに、当該結果を反映した共通キャリア・スキルフレームワークの普及浸透を図る。

(ク) 情報セキュリティ資格の周知及び普及 （内閣官房、総務省及び経済産業省）

a) 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。

b) 内閣官房、総務省及び経済産業省において、民間における情報セキュリティ専門家の充実の観点から、民間の情報セキュリティに関する資格及び教育プログラムについて一層の周知及び普及を図る。

(ケ) 情報セキュリティに関する国家試験の改善 （経済産業省）

経済産業省において、昨今の情報セキュリティの重要性の一層の高まりや情報セキュリティ人材が不足している状況を踏まえ、情報セキュリティスペシャリスト試験を含む情報処理技術者試験の全試験区分を対象に、情報セキュリティに関する出題の強化・拡充を実施する。

(コ) 情報処理技術者試験制度に関する在り方についての検討 （経済産業省）

情報セキュリティに対する実践的能力を常に評価・担保できる試験、資格・認証制度として位置付けられるよう、例えば海外の民間資格のように合格後に継続教育を設けるとともに、情報セキュリティ人材の能力を認証する等、試験制度に関する在り方についての検討を進める。

(サ) IT スキル標準の活用（公共機関での活用を含む） （経済産業省）

経済産業省において、IPA において整備・普及をすすめている IT スキル標準を活用し、実践的な教育プログラム等に関する大学等専門教育課程の充実化、産学連携の強化などセキュリティレベルに対応した多様な資格・能力評価制度の在り方などを検討し、結論を得る。

（シ）グローバル水準の人材の育成 （内閣官房及び関係府省庁）

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。

（ス）大学に対する情報セキュリティに関する最新情報の提供 （内閣官房、総務省、文部科学省及び経済産業省）※再掲

内閣官房、総務省、文部科学省及び経済産業省において、大学における情報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。

（セ）サイバー攻撃の事例共有、ケースを基にした教材等の開発 （内閣官房及び関係省庁）

行政機関等が入手した情報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、関係者の同意等を得た上で、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。

（ソ）情報セキュリティに関する教員の養成 （内閣官房、総務省、文部科学省及び経済産業省）

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。

（タ）情報セキュリティ監査知識を有する人材の育成等の促進 （内閣官房及び経済産業省）

内閣官房及び経済産業省において、情報セキュリティ対策を組織の内部及び外部から客観的かつ公正に評価できる情報セキュリティ監査知識を有する人材の育成を行う。

（チ）情報セキュリティ人材育成に係る枠組みの検討 （経済産業省）

a) 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 人材の育成のため、産学が自立的かつ継続的に実施するためのプラットフォーム構築に向け、引き続き検討するなど、産学連携体制を強化する。

b) 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。

c) 経済産業省において、共通キャリア・スキルフレームワークに基づき、情報セキュリティ人材を含めた高度 IT 技術者のスキル標準を一層高度化し普及浸透を図る。

d) 経済産業省において、アジアでの更なるセキュリティ人材の育成を図るため、アジア 11 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)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 の取組を拡大するとともに、我が国の IT スキル標準を普及させていく。

(ツ) 制御システムセキュリティに係る人材育成 （経済産業省）

経済産業省において、CSSC のテストベッド施設を活用し、制御システムセキュリティに係る人材育成のための研修等を実施する。

(テ) 政府機関等による民間セキュリティ人材の一時的受入れ （内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、政府機関や独立行政法人等がハブとなり産学官のセキュリティ関連業務を交互に経験できる機会を設けることなどにより、幅広いネットワークの形成を図り、情報セキュリティ人材を育成する。

(ト) 優秀な外部人材の活用 （内閣官房及び関係府省庁）※再掲

内閣官房において、優秀な外部人材の活用に関する事例を収集し、情報提供を行うなど、各府省庁と協力し、官民の人事交流等により情報セキュリティに係る外部人材の活用を進める。

④ リテラシー向上

【 初等中等教育段階における取組 】

(ア) 初等中等教育段階における情報に関する教育 （文部科学省）

a) 文部科学省において、現行の学習指導要領を踏まえ、発達段階に応じ、情報セキュリティを含む情報モラルに関する教育を積極的に推進する。

b) 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の活用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、各地域で情報教育を推進する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。

【 高齢者層などリテラシーの強化が必要とされる層における対策 】

(イ) 情報セキュリティ・サポーターの育成・活用 （総務省）

総務省において、利用者の身近なところで利用者を支援する情報セキュリティに詳しい人（情報セキュリティ・サポーター）を育成・活用する活動を支援し、国民全体の情報セキュリティの底上げを行う。

(ウ) 情報セキュリティ相談窓口の充実 （内閣官房及び関係府省庁）

内閣官房において、各府省庁と協力し、各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。

【 スマートデバイスへの対応 】

(エ) スマートフォン等による安心・安全な無線 LAN の利用の推進 （総務省）

総務省において、スマートフォン等の普及により急増するモバイルトラヒックに対処するため、利用者が適切な情報セキュリティを確保しながら、無線 LAN にオフロードする方策を引き続き検討し、電波の能率的な利用を促進する。

(オ) 官民連携によるスマートフォン等の情報セキュリティ確保の推進 （総務省及び経済産業省）

a) 総務省及び経済産業省において、スマートフォン等の普及に伴って情報セキュリティ上発生する問題点について、官民連携しつつ技術的な課題等について、必要な対策を講じる。

b) 総務省及び経済産業省において、政府や事業者等における技術的対策、サービス運用面での対策、利用者への普及啓発の取組等を適宜取りまとめ、情報を発信する。

(カ) スマートフォン等におけるフィルタリングの在り方の検討 （総務省及び経済産業省）

総務省及び経済産業省において、スマートフォン等に対応したフィルタリングの改善等に向け、関係事業者との調整に取り組む。

(キ) スマートフォン時代における利用者情報保護に関する取組の推進 （総務省）

総務省で取りまとめた SPI[25]及び SPIⅡ[26]を踏まえ、アプリケーションのプライバシーポリシーの作成・公表を一層促進する。また、アプリ事業者等に対する情報提供・周知啓発等、総合的な利用者保護に関する取組を推進するとともに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みの構築に引き続き取り組む。

(ク) ソーシャルメディアの利用に係る情報セキュリティ確保方策 （総務省及び経済産業省）

総務省及び経済産業省において、近年のソーシャルメディアの利用拡大に伴い、情報セキュリティ上の課題も増加していることから、ソーシャルメディアの利用において情報セキュリティ上の観点から留意すべき事項等について周知を図る。

[25] スマートフォン プライバシー イニシアティブ（Smartphone Privacy Initiative）の略。2012 年８月「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」提言。
[26] スマートフォン プライバシー イニシアティブⅡ（Smartphone Privacy Initiative Ⅱ）の略。2013 年９月「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」提言（スマートフォン安心安全強化戦略の第Ⅰ部）。

3 「世界を率先する」サイバー空間の構築

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

2014 年度においては、「サイバーセキュリティ戦略」を受けて 2013 年 10 月に策定された「サイバーセキュリティ国際連携取組方針」に則り、サイバー空間における各国との国際連携・協調体制の構築による事案対処能力の向上、サイバー空間の安定的利用を確保するための国際的なルール作りの推進等に繋がる施策を具体化してゆく。

① 外交

【 基本的な価値観を共有する国等との多角的なパートナーシップの構築・強化 】

(ア) ハイレベルによる戦略的な取組の強化 （内閣官房、外務省及び関係府省庁）

内閣官房、外務省及び関係府省庁において、サイバー空間に関する国際的な議論の場で、我が国の基本的な価値観が国際的な規範作りに最大限に反映されるよう、ハイレベルによる働き掛け・取組の強化を行う。

【 従来の国際法の適用に関する検討の深化 】

(イ) サイバー空間に関する国際的な規範作りへの参画等 （内閣官房、総務省、外務省、経済産業省及び関係府省庁）

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、活発化するサイバー空間に関する国際的な議論に対して、二国間の協議・意見交換、国際会議などのマルチの場を活用し、サイバー空間を利用した行為に対する従来の国際法の適用に関する議論や国際的な規範作りに積極的に関与する。

(ウ) 「国際安全保障の文脈における情報及び電気通信分野の進展」に関する政府専門家会合への政府専門家の派遣等による安全保障分野での国際議論への参画 （内閣官房、外務省及び関係府省庁）

内閣官房、外務省及び関係府省庁において、国連からの要請による、国連総会決議「国際安全保障の文脈における情報及び電気通信分野の進展」に基づき設置される政府専門家会合に対し、我が国から政府専門家を派遣する等、安全保障面での脅威認識やサイバーセキュリティ分野における行動規範作り、信頼醸成措置の促進及び能力構築支援などについて積極的に寄与する。

【 二国間・多国間の協議・対話等の継続・拡大 】

(エ) サイバーセキュリティ政策に関する二国間対話の強化 （内閣官房、総務省、外務省、経済産業省及び関係府省庁）

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、日米サイバー対話、インターネットエコノミーに関する日米政策協力対話等の二国間会合等を開催し、政府一体となった関与を一層強めるような枠組みの構築を通じてサイバーセキュリティに関する個別分野における連携について協議するなどして、米国との連携強化を図る。

また、日英サイバー協議や日 EU インターネット・セキュリティフォーラムを開催するほか、日露サイバー安全保障協議の立ち上げ、エストニアとのサイバー協議立ち上げ、フランスとのサイバー対話立ち上げ、日 EU サイバー対話の立ち上げ、日 EU ICT 政策対話等の開催などを通じ、欧州諸国ともサイバーセキュリティ分野に関する協力体制の構築に向けた議論を行う。

加えて、インドと日印サイバー協議を開催するほか、日豪サイバー協議の立ち上げなどを通じ、アジア太平洋諸国とのサイバーセキュリティ分野に関する情報交換、協議等も積極的に行う。

(オ) 海外情報セキュリティ機関との情報交換 （経済産業省）

経済産業省において、NIST、韓国インターネット振興院（KISA）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。

(カ) 多国間の枠組み等における国際連携・協力の推進 （内閣官房、外務省及び関係府省庁）

内閣官房及び関係府省庁において、Meridian 等の重要情報インフラ防護に係る分野、APEC、OECD 等のグローバルな経済活動に係る分野、IWWN 等の国際的な情報共有等に関する分野、FIRST 等のインシデント対応に係る分野、国連や ARF 等の国家安全保障に係る分野、ITU や APT 等の情報通信に係る分野、国際犯罪防止刑事司法委員会や G8 ローマ・リヨン・グループ等のサイバー犯罪対策に係る分野等の様々な分野の国際会合に積極的に参加し、重要インフラ防護、標準化を含むグローバルな取組、インシデント対応、サイバー攻撃への対応等に関して積極的な情報共有を行う。

2014 年 11 月には Meridian 会合を我が国で開催することとしており、重要インフラ防護等、サイバー空間における各分野の課題等に対する国際協調・協力に積極的に寄与する。

【 日米安保体制を基軸とした米国との協力の深化 】

(キ) サイバー空間における米国との協力の深化 （内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係府省庁）

2013 年５月に続き、2014 年４月に開催された日米サイバー対話において、両国におけるサイバー空間に関する幅広い能力を深化させ、日米同盟を強化させるため、サイバー空間に関する脅威情報の交換、国際的なサイバー政策についての連携、それぞれのサイバー戦略の比較、重要インフラに対する共通の脅威に対抗するための取組や計画における協力、及び防衛・安全保障政策におけるサイバーセキュリティ分野の協力について議論が行われたことを踏まえ、サイバー空間における更なる日米協力の深化を図る。

② 国際展開

【 ASEAN 地域等とともに成長できる関係の構築 】

(ア) 日・ASEAN 情報セキュリティ政策会議の推進による日・ASEAN 関係の連携強化 （内閣官房、総務省、外務省及び経済産業省）

内閣官房、総務省、外務省及び経済産業省において、我が国との経済関係の深化が進むアジア地域におけるセキュアなビジネス環境の構築、経済活動・技術革新を支える情報通信インフラの信頼性の確保、政府による横断的な情報セキュリティ政策の立案に向けた取組を加速化するため、日・ASEAN 情報セキュリティ政策会議を通じ ASEAN 諸国との連携を強化する。

a) 内閣官房、総務省及び経済産業省において、第６回日・ASEAN 情報セキュリティ政策会議の決定事項を着実に推進する。

b) 内閣官房、総務省及び経済産業省において、第７回日・ASEAN 情報セキュリティ政策会議を日本で開催する。

c) 内閣官房において、第６回日・ASEAN 政府ネットワークセキュリティワークショップをシンガポールで開催する。

d) 内閣官房、総務省及び経済産業省において、ASEAN 諸国との情報セキュリティ意識啓発共同事業、サイバー連絡演習及び専門家パネルによる具体的協力分野の検討等を実施する。

e) 内閣官房、総務省、外務省及び経済産業省において、他の ASEAN 諸国への効果波及にも留意しつつインドネシアに対する情報セキュリティ能力向上のための技術協力プロジェクトを実施する。

f) 内閣官房及び総務省において、ワークショップの開催等を通じて、我が国と ASEAN 加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進する。

g) 内閣官房、総務省及び経済産業省において、研究や技術面での連携に資するため、我が国と ASEAN 加盟国におけるネットワークセキュリティ分野の専門家の交流を促進する。

(イ) 日・ASEAN のサイバー犯罪対策協力の促進 （警察庁及び外務省）

第１回日・ASEAN サイバー犯罪対策対話を開催する。右枠組みを通じて、サイバー犯罪対策分野において、日・ASEAN 間の情報共有及び連携を促進するとともに、ASEAN 諸国のサイバー犯罪対策能力構築支援を行う。

(ウ) 国際連携を活用した国内外における普及・啓発活動の実施 （内閣官房及び関係府省庁）※再掲

内閣官房及び関係府省庁において、ASEAN、欧米を始めとする諸国と国際連携を活用した行事や情報セキュリティ対策に関する情報提供等を行う「情報セキュリティ国際キャンペーン」を実施し、国際連携の一層の推進と、国内における情報セキュリティ対策の更なる普及・啓発を図る。

(エ) APEC における情報セキュリティ分野の連携推進 （総務省及び経済産業省）

a) 総務省及び経済産業省において、APEC 電気通信・情報産業大臣会合で定められた、情報通信分野に関して APEC として目指すべき共通目標において、安全・信頼性のある ICT 環境の推進が含まれていることを踏まえて、我が国と APEC 域内各国・地域との間でネットワークセキュリティ分野における研究開発や意識啓発等の連携を推進する。

b) 経済産業省において、JPCERT/CC を通じ、我が国の CSIRT 構築支援活動の経験の蓄積を活かし、APCERT 等の国際枠組みに協力の呼びかけを行い、ニーズのある APEC 域内各国・地域に対し、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。

(オ) 海外の組織内 CSIRT の構築・運用支援 （経済産業省）

経済産業省において、JPCERT/CC を通じ、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、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。

(カ) 各国における対外・対内調整を担う CSIRT の体制強化の支援及び連携の強化 （経済産業省）

a) 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 における CSIRT 構築支援活動の経験の蓄積をもとに、インシデント対応業務の運用技術や CSIRT 間連携／運用に関する経験の共有やサイバー演習の実施のためのツールの提供等の支援を行う。

b) 経済産業省において、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、JPCERT/CC を通じ、各国 CSIRT と JPCERT/CC とのインシデント対応に関する連携を一層強化する。

(キ) ASEAN のビジネス環境整備（ISMS 等） （経済産業省）

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や、IPA において整備・推進している情報セキュリティ対策ベンチマーク等のツールの技術提供と導入の支援を実施する。

(ク) サイバー攻撃事前防止・早期対策に向けた取組の推進 （総務省）※再掲

a) 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ネットワークを国際的に構築し、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。

b) 総務省において、米国とは、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、サイバー攻撃に関するデータを共有し、研究開発の分野での協力関係を加速化していくべきであるということで一致したことを踏まえ、サイバー攻撃の予兆を検知し迅速

に対応することを可能とする技術の研究開発等を効果的に実施するため、データの共有を開始しているところであり、引き続き、米国との情報共有を強化する。

c) 総務省において、EU とは、引き続き、ネットワーク上の攻撃の軽減のための共同研究の実施等の課題について議論を進める。

d) 総務省において、ASEAN 諸国との連携プロジェクトである JASPER による連携を推進する。

(ケ) アジア太平洋地域等での早期警戒情報の共有促進 （経済産業省）

a) 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。

b) 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の構築に資する開発、運用協力体制の検討を進める。

(コ) 途上国向け研修・セミナー等の開催 （総務省）

総務省において、ネットワークセキュリティ分野における APT 加盟国等との国際連携を考慮し、当該国の政府関係者及び電気通信事業者等を対象として、情報セキュリティの動向、技術、政策等に関する研修やセミナー等を実施する。

(サ) 途上国に対する技術援助の推進（サイバー犯罪対策のための刑事司法制度整備） （警察庁、法務省及び外務省）

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。

(シ) ソフトウェア開発のアウトソーシング先国等におけるセキュアコーディングセミナーの実施 （経済産業省）

経済産業省において、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 JPCERT/CC 開催の技術セミナーを実施する。

【 日本企業の国際展開の促進 】

(ス) 情報セキュリティ分野での国際標準化への参画 （総務省及び経済産業省）

a) 総務省において、NICT とともに、情報セキュリティ分野の国際標準化活動である ITU-T

SG17、ISO/IEC JTC1/SC27 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。

b) 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。

(セ) 脆弱性対策に関する国際標準化活動等への参画 （経済産業省）

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。

(ソ) Common Criteria（ISO/IEC15408）における国際協調 （経済産業省）

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。

(タ) ハードウェア CC 評価・認証制度における欧州との協調関係の構築 （経済産業省）

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。

(チ) 制御システムセキュリティに関する国際支援 （経済産業省）

経済産業省において、CSSC を中心として、日本産業が強みを持つ分野について、制御システムセキュリティに係る評価・認証の標準化をリードし、各国にも受け入れられるよう働きかけ、協力関係構築を強化する。

(ツ) 制御システムのセキュリティに係る米国との連携推進 （経済産業省）

経済産業省において、米国等との間で制御システムセキュリティに関する評価・認証の相互承認の推進や CSSC のテストベッド施設の運用及び訓練の実施を含む人材育成のための情報共有など、制御システムセキュリティに係る連携を推進する。

(テ) 国際的なルールに基づくセキュリティ製品の貿易の推進 （経済産業省）※再掲

経済産業省において、日本が強みを持つ複合機や制御システム等の日本製品が貿易において不利な扱いを受けることがないよう、IPA を通じ、セキュリティの国際標準化や評価・認証の国際的な相互承認枠組みに積極的に参画、働きかけを進める。

（ト）個人情報の保護に関する国際的な取組への対応 （消費者庁）

消費者庁において、OECD 情報コンピュータ通信政策委員会情報セキュリティプライバシーワーキンググループ会合、APEC 電子商取引運営委員会データプライバシーサブグループ会合等に出席し、OECD におけるプライバシー法執行の越境的な課題の検討や APEC データ・プライバシー・パスファインダー・プロジェクト等の取組を把握し、国際的な協調の観点から我が国として必要な対応・措置を検討するとともに、我が国の個人情報保護関連法制等について国際的な理解を求める。

③ 国際連携

【 サイバー犯罪対策における連携 】

(ア) サイバー攻撃に関する諸外国関係機関との連携の強化 （警察庁及び法務省）

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。

(イ) サイバー犯罪の取締りのための国際連携の推進 （警察庁）

警察庁において、我が国のサイバー犯罪情勢に関係の深い国々の法執行機関それぞれとの効果的な情報交換を実施するとともに、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、外国捜査機関等とのサイバー犯罪に関する情報交換を継続的に行うとともに、サイバー犯罪に関する最新の捜査手法を修得し、外国捜査機関との連携を強化するため、職員を派遣する。

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

(ウ) 中央当局制度を活用した国際捜査共助の迅速化 （警察庁及び法務省）

警察庁及び法務省において、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) サイバー犯罪条約普及への参画 （外務省）

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、引き続き同条約ビューローメンバーとして同条約の普及等に積極的に参画する。

【 情報共有・信頼醸成措置の推進 】

(オ) 国際会議等への参加を通じた連携の強化 （内閣官房、警察庁、総務省、経済産業省及び関係府省庁）

内閣官房、警察庁、総務省、経済産業省及び関係府省庁において、サイバー攻撃への対応能力を向上させるため、IWWN や FIRST 等の国際連携枠組みへの参加を通じて、諸外国との連携強化を推進する。

インシデント対応調整や脅威情報の共有等、サイバー攻撃への対応能力を向上させるため、

JPCERT/CC を通じ、FIRST 等の国際連携枠組みへの参加により、諸外国との連携強化を推進する。

(カ) 諸外国との CSIRT 間連携の強化 （経済産業省）

インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口としての JPCERT/CC の機能強化を図るとともに、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。

(キ) 国際的な窓口機能の強化を通じた各国との連携 （内閣官房）

a) 内閣官房において、国際的な PoC として、情報セキュリティ先進国である我が国の情報セキュリティ政策の基本理念や戦略、官民等のベストプラクティスに関する国際的な広報、情報発信に努める。

b) 内閣官房において、会議等で把握した情報セキュリティ政策に関する国際機関や標準化の動向、海外のベストプラクティス、脅威・脆弱性に関する情報等を国内の関係機関等と共有、還元する。

4 推進体制等

(ア) NISC の機能強化　（内閣官房）

内閣官房において、関係府省庁と協力し、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組に向けて、NISC の機能強化等に関する方針を策定し、同方針に基づき所要の措置を講じる。

(イ) 関係機関等との連携強化　（内閣官房及び内閣府）

内閣官房及び内閣府において、IT 総合戦略本部はもとより、総合科学技術・イノベーション会議、中央防災会議、知的財産戦略本部等、関係する本部・会議との連携を密にし、様々な方策の提案や実施において緊密に協力し、政府全体として情報セキュリティ政策を一体的に推進する。

(ウ) 情報セキュリティ対策に資する各種ツール・分析等の提供　（経済産業省）

セキュリティ対策・プライバシーに関する状況の調査・分析を行うとともに、「情報セキュリティ白書 2014」の編集、作成、出版等を IPA を通じて実施する。

(エ) 官民の情報共有の更なる推進　（内閣官房及び関係府省庁）

内閣官房は各府省庁が運用する官民の情報共有ネットワークと政府機関の情報共有ネットワークの結節点の役割を果たすことにより、サイバー攻撃に関する官民の情報共有の更なる推進を図る。

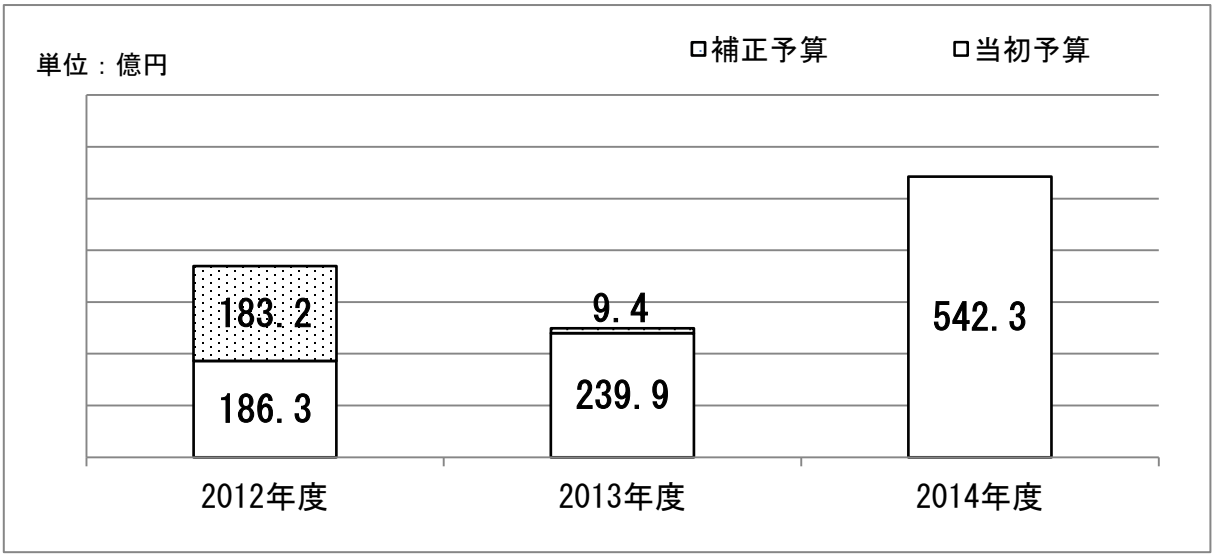
(オ) サイバー攻撃に関するインシデント情報等の政府機関や重要インフラ事業者等の関係機関間における共有の促進　（内閣官房）

内閣官房において、関係府省庁と協力し、サイバー攻撃に関するインシデント情報等の政府機関や重要インフラ事業者等の関係機関間における共有を促進するための秘密の保持の枠組みについて、2015 年度を目途とする「サイバーセキュリティセンター」（仮称）への改組と合わせて整備するため、既存の仕組みの活用の在り方、共有する目的、共有される情報等の内容や共有する者の範囲等の検討を行い、結論を得、可能なものから順次、実施する。

資料１　政府のサイバーセキュリティ関係予算額の推移

	2012 年度	2013 年度	2014 年度
当初予算額	186.3 億円	239.9 億円	542.3 億円
補正予算額	183.2 億円	9.4 億円	―

※ 情報セキュリティに関する予算として切り分けられないものは計上していない。
※ 補正には減額補正を含む。



資料２　用語解説

	用　語	解　説
A	AIST	national institute of Advanced Industrial Science and Technology の略。独立行政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。
	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。
	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。
	ARF	ASEAN Regional Forum の略。政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラム。
	ASEAN	Association of South East Asian Nations の略。東南アジア諸国連合。
B	BCP	Business Continuity Plan の略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、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。
	BEMS	Building Energy Management System の略。業務用ビル等において、室内環境・エネルギー使用状況等を把握し、室内環境に応じた機器、設備等の運転管理によってエネルギー消費量の削減を図るシステム。
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。
	CIO	Chief Information Officer の略。「情報化統括責任者」。企業や行政機関等の組織において情報化戦略を立案、実行する責任者のこと。なお、「政府CIO」は内閣情報通信政策監である。
	CISO	Chief Information Security Officer の略。「最高情報セキュリティ責任者」。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣官房情報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。
	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。
	CYREC	Cybersecurity Research Center の略。標的型攻撃等の新たなサイバー攻撃の抜本的な解決を目指し、2013年4月、NICTが主導的な役割を担って構築した、オール・ジャパンの英知を結集したサイバーセキュリティ研究開発拠点。
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。
	DKIM	DomainKeys Identified Mail の略。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールにおける送信元のなりすまし等を防ぐ。
E	EU	European Union の略。欧州連合。
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、2014年５月現在、世界64ヶ国の官・民・大学等298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。
	GPKI	Government Public Key Infrastructure の略。国民等から行政機関に対する申請・届出等や、行政機関から国民等への申請・届出等に対する結果の通知等を、インターネットを利用しペーパーレスで行うことを目的として、申請・届出等やその結果の通知等が、真にその名義人（申請者や行政機関の処分権者）によって作成されたものか、申請書や通知文書の内容が改ざんされていないかを確認する行政機関側の仕組みとして整備された公開鍵暗号方式によるデジタル署名を用いた認証システム。
	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。内閣官房情報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	ICPO	International Criminal Police Organization の略。国際刑事警察機構。
	ICSR	Industrial Control System Security Response Group の略。2012年７月に起ち上げたJPCERT/CCの制御システムセキュリティ対策グループのこと。
	ICT	Information and Communications Technology の略。情報通信技術のこと。
	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。
	ISO/IEC 15408	CC（Common Criteria）を参照。
	ISO/IEC 27000シリーズ	情報セキュリティの管理・リスク・制御に関するベストプラクティスを提供する国際規格。

	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。
	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	JASPER	Japan-ASEAN Security PartnERshipの略。ASEAN各国向けのセキュリティ対策に関する総合的な技術協力プロジェクト。
	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。標的型攻撃の未然防止及び被害拡大防止のため、重要インフラ機器製造業、電力、ガス、石油、化学の業種について、IPAを情報集約点とした情報共有、早期対応を行う枠組のこと。2011年10月に発足し、2012年４月より本格運用開始。
	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。
K	KISA	Korea Internet & Security Agency の略。韓国インターネット振興院
L	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。

	Meridian	重要インフラ防護に関する国際連携を推進する場として、2005年にイギリスで開始された会合。欧米諸国やアジア各国等の政府機関（重要インフラ防護担当）が参加し、ベストプラクティスの交換や国際連携の方策などについて議論している。
	MOU/NDA	Memorandum Of Understanding/Non-Disclosure Agreement の略。覚書及び秘密保持契約。
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。独立行政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。
	NISC	National Information Security Center の略。内閣官房情報セキュリティセンター。2005年に情報セキュリティ政策に係る基本戦略の立案その他官民における統一的、横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行うために設置。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。
	PDCAサイクル	Plan-Do-Check-Act cycle。事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つ。Plan（計画）→Do（実行）→Check（評価）→Act（改善）の４段階を繰り返すことによって、業務を継続的に改善する。
	PoC	Point of Contact の略。連絡窓口。
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。
	SEC	Securities and Exchange Commission の略。米国証券取引委員会。
	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。
	SPF	Sender Policy Framework の略。電子メールにおける送信ドメイン認証の一つ。差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる。
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。
	暗号化	第三者に容易に解読されないよう、定められた規則に従ってデータを変換すること。
	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により運用される。

お	オープンデータ	行政機関が保有する統計・行政などのデータを広く利用しやすい形で公開すること。Data.gov（米国）やData.gov.uk（英国）などの取組が各国政府によって行われており、我が国でも電子行政オープンデータ戦略が策定され、取組が進んでいる。
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。
	各府省情報化統括責任者（CIO）連絡会議	政府全体として情報化推進体制を確立し、行政の情報化等を一層推進することにより国民の利便性の向上を図るとともに、行政運営の簡素化、効率化、信頼性及び透明性の向上に資するため、2002年９月、IT総合戦略本部に設置された会議。政府CIOを議長とする。
	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）
	業務継続計画	BCPを参照。
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新しいコンピュータ・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。
こ	コンピュータウィルス	自分自身の複写、又は自分自身を変更した複写を他のプログラムに組み込むことによって繁殖し、感染したプログラムを起動すると実行されるプログラム。マルウェアと同義としても用いられる。
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。
	サイバー攻撃解析協議会	サイバー攻撃の実態を把握し、その結果を関係省庁、重要インフラ事業者等に提供することを目的に、総務省、経済産業省、NICT、IPA、テレコム・アイザック推進会議、JPCERT/CCにより2012年７月に発足した協議会。
	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	事案対処省庁	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。警察庁、消防庁、海上保安庁及び防衛省。
	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。
	情報セキュリティガバナンス協議会	企業組織が適切な情報セキュリティガバナンスを確立することを促進するため、経営陣が情報リスクについて正しく理解し、組織として適切なリスク管理と情報セキュリティ対策を実施することを目指し、情報リスクの管理に関する知見の共有や情報セキュリティガバナンスに関する普及啓発等を実施することを目的に2012年５月21日に設立された協議会。
	情報セキュリティ関係省庁	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。警察庁、総務省、外務省、経済産業省及び防衛省。
す	スパムメール	迷惑メールのこと。

	スマートコミュニティ	様々な需要家が参加する一定規模のコミュニティの中で、再生可能エネルギーやコージェネレーション等の分散型エネルギーを用いつつ、ＩＴや蓄電池等の技術を活用したエネルギーマネジメントシステムを通じて、分散型エネルギーシステムにおけるエネルギー需給を総合的に管理し、エネルギーの利活用を最適化するとともに、高齢者の見守りなど他の生活支援サービスも取り込んだ新たな社会システムを構築したもの。
	スマートデバイス	情報処理端末のうち、単なる計算処理だけではなく、多用途に使用可能な多機能端末のこと。スマートフォンやタブレット端末の総称として使われることが多い。
	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	通信機能を備え、電力使用量などを自動送信したり、家電製品等を制御可能な次世代の電力メーター。
せ	政府機関統一基準群	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。
	政府共通プラットフォーム	各府省が別々に整備・運用している政府情報システムを可能なものから順次統合・集約化し、政府情報システム全体の運用コストの削減、セキュリティの強化等を図るための基盤。2013年３月から運用開始。
	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。
	セプター	CEPTOAR （Capability for Engineering of Protection, Technical Operation, Analysis and Response の略）。重要インフラ分野における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、2013年末現在、10分野で15セプターが活動。
	セプターカウンシル	CEPTOAR-Council。各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
そ	ソーシャルメディア	ブログ、ソーシャルネットワーキングサービス（SNS）、動画共有サイトなど、利用者が情報を発信し、形成していくメディア。利用者同士のつながりを促進する様々なしかけが用意されており、互いの関係を視覚的に把握しやすいのが特徴。
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。
ち	中央当局制度	特定の当局を中央当局として指定し、外交ルートを経由せずに中央当局間で共助の授受を行う制度。
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、また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（Telecom Information Sharing and Analysis Center Japan）。通信事業者等が中心となって設立した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。

	テレワーク	ICTを活用して、場所と時間にとらわれない柔軟な働き方。企業等に勤務する被雇用者が行う雇用型テレワーク（例：住宅勤務、モバイルワーク、サテライトオフィス等での勤務）と、個人事業者・小規模事業者等が行う自営型テレワーク（例：SOHO、住宅ワーク）に大別される。
	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	ドメイン名	国、組織、サービス等の単位で割り当てられたインターネット上の名前であり、英数字等を用いて表したもの。
な	内閣官房情報セキュリティセンター	2005年に情報セキュリティ政策に係る基本戦略の立案その他官民における統一的、横断的な情報セキュリティ対策の推進に係る企画及び立案並びに総合調整を行うために設置。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 Information Security Center）。
	なりすまし	他の利用者のふりをすること。または、中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。
は	ハッカー	コンピュータ技術に長けた人のこと。または、コンピュータ技術を利用して、ハッキングを行う人のこと。悪意を持って、コンピュータの不正利用や攻撃を行う人のことをハッカーと呼ぶこともあるが、本来は、悪い意味の言葉ではない。そのような悪意を持った人は、本来はクラッカーという。
	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。
	フィッシング対策推進連絡会	フィッシングに関する情報の共有を図るとともに、その効果的な対策について検討することを目的として、電気通信事業者等を構成員として2005年１月に設置された連絡会。
	フィルタリング	インターネットのウェブページ等を一定の基準で評価判別し、違法・有害なウェブページ等の選択的な排除等を行う機能のこと。
	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。
へ	ベストプラクティス	優れていると考えられている事例やプロセス、ノウハウなど。

ほ	ポート	ポート番号。コンピュータが通信する際に通信先のプログラムを識別するための番号で、通常利用されるTCP/IPでは、65535番まである。通常、プロトコルに応じてポートが割り当てられている。たとえば、FTPはTCPの21番ポート（制御用）と20番ポート（データ用）、HTTPはTCPの80番ポート、HTTPSはTCPの443番ポートを使用する。
	ボットウィルス	コンピュータを外部から遠隔操作するためのプログラムの一種。ボットウィルスに感染してしまうと、外部からの指示を待ち、インターネットを通じて、攻撃者にコンピュータを遠隔操作されてしまう。外部から遠隔操作するという動作から、ロボット（Robot）をもじってボット（BOT）と呼んでいる。
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。
む	無線LAN	無線通信で情報を送受信する通信回線。IEEE802.11a、802.11b、802.11g、802.11n、802.11ac等の規格がある。
め	迷惑メール対策推進協議会	電気通信事業者、送信事業者、広告事業者、配信ASP事業者、セキュリティベンダー、各関係団体、消費者、学識経験者、関係省庁など迷惑メール対策に関わる関係者が幅広く集まり、関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などにより、関係者による効果的な迷惑メール対策の推進に資することを目的として、2008年11月27日に設立された協議会。
	迷惑メール追放支援プロジェクト	民間事業者による自主的な迷惑メール対策を促すことを目的とした取組。2005年２月から開始。
り	リカレント教育	職業人を中心とした社会人に対して、学校教育の修了後、いったん社会に出てから行われる教育であり、職場から離れて行われるフルタイムの再教育のみならず、職業に就きながら行われるパートタイムの教育も含む。