資料３－１

政府における情報セキュリティ政策の動きについて

平成25年7月５日（金）
情報セキュリティ アドバイザリーボード

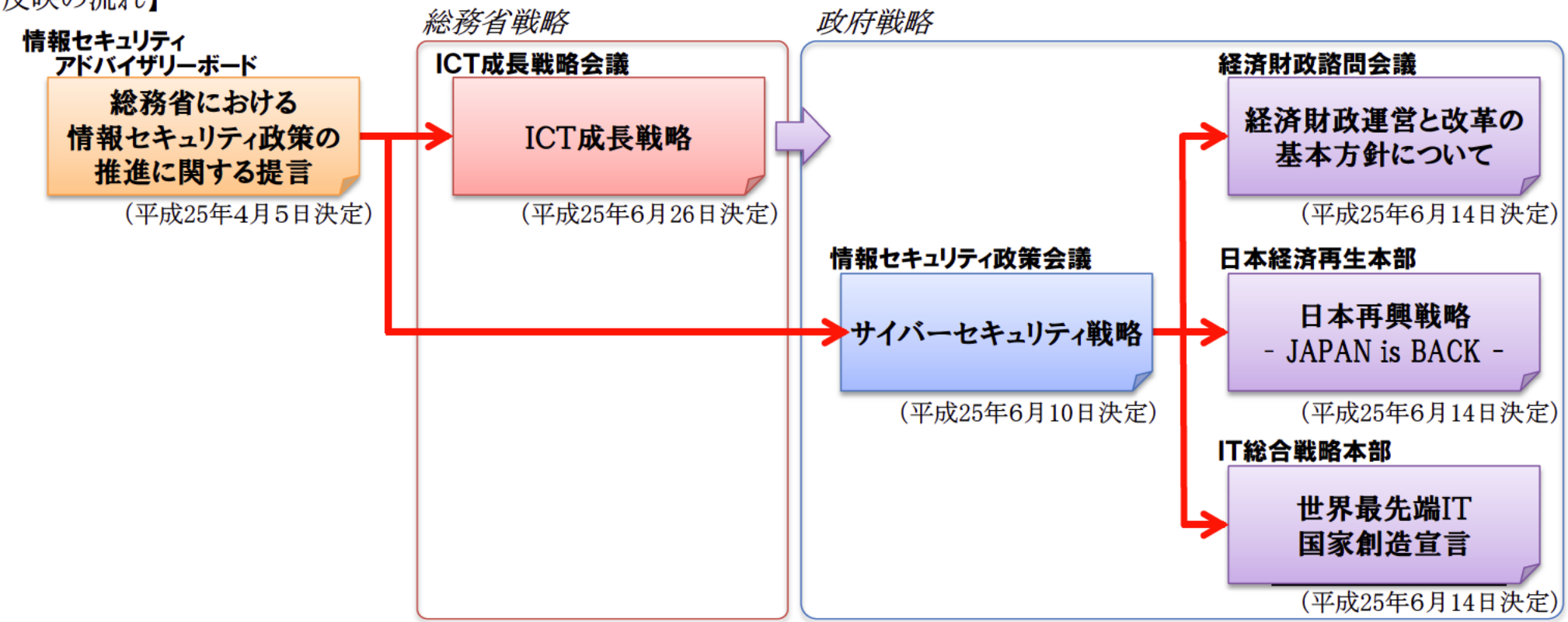
「総務省における情報セキュリティ政策の推進に関する提言」の政府戦略への反映

「情報セキュリティ　アドバイザリーボード」では、情報セキュリティを取り巻く環境の変化に迅速かつ的確に対応するための取組の方向性として、「総務省における情報セキュリティ政策の推進に関する提言」(平成25年４月５日公表)を取りまとめ。

本提言に基づき、情報セキュリティ政策の基本的な考え方、方策等を、「ICT成長戦略会議」(総務省)及び「情報セキュリティ政策会議」(議長:内閣官房長官)に提案し、「ICT成長戦略」(平成25年６月26日　総務省決定)及び政府の基本戦略である「サイバーセキュリティ戦略」(平成25年６月10日 情報セキュリティ政策会議決定)に反映。

また、「経済財政運営と改革の基本方針について」(平成25年６月14日　閣議決定)、「日本再興戦略　-JAPAN is BACK-」(平成25年６月14日　閣議決定)及び「世界最先端IT国家創造宣言」(平成25年６月14日　閣議決定)においても、サイバーセキュリティ政策の推進について記載。

【反映の流れ】



１.「ICT成長戦略」への反映

ICT成長戦略　－施策の全体像－

主に産学官で実施するプロジェクト

社会的課題の解決

超高齢社会 × ICT

○「スマートプラチナ社会」構築
- ＩＣＴ健康モデル（予防）の確立
  （➢2016年度までに有効な方策を確立）
- 医療情報連携基盤の全国展開
  （➢2018年度までに全国へ普及・展開）
- ＩＣＴリテラシーの向上

○女性等の活力発揮のためのテレワーク推進
（➢テレワーク導入企業を2020年に2012年度比3倍）

【2020年までに23兆円規模の新産業創出】

資源問題 × ICT

【鉱物・エネルギー、水、農業、社会インフラ】

○衛星を活用した「海のブロードバンド」の実現
（海底資源調査の高度化・効率化）

○高度な漏水検知システム等の展開【海外展開】

○農業の知識産業化、バリューチェーン構築
（➢2020年度には農林水産物輸出目標1兆円に貢献）

○道路・橋梁等の効率的な維持管理の実現
（➢2020年度までにインフラの20%はセンサー等を活用）

【2025年までに約20兆円の経済効果】

新たな付加価値産業の創出

放送コンテンツの海外展開

○権利処理の効率化・迅速化、海外市場拡大の促進【海外展開】

◆推進体制の整備

【2018年までに現在の3倍の海外事業売上高】

放送サービスの高度化

○次世代放送システムの早期実現
（4K・8K、スマートテレビ）

➢放送開始:4K、スマテレ→2014年、8K→2016年
➢市販のテレビでの放送環境実現→2020年

◆推進体制の整備
◆ロードマップの作成

ICTによるイノベーション創出

○ITSパイロットプロジェクトの推進

G空間 × ICT

○G空間オープンデータ・プラットフォームの構築
○世界最先端のG空間防災システムの構築
○「G空間シティ（仮称）」による成功モデルの実現

➢多様なメディアを活用した情報収集・伝達手段を2015年度までに構築
➢G空間情報を利用した消火活動を2020年度までに導入

【2020年に約62兆円のG空間関連市場】

街づくり × ICT

○「ICTスマートタウン」実証プロジェクトの展開・加速化

主に国が実施する環境整備

街づくり × ICT

○共通プラットフォームの構築 ⇐ 成果展開（～2018年）のための体制整備

ICTによるイノベーション創出

○技術成果の具現化を支援する常時応募可能な公募制度の新設
○独創的な人向けチャレンジ枠の創設

情報セキュリティ

○サイバーセキュリティ研究開発拠点（CYREC）の構築による解析能力の向上
○国際連携の推進（日・ASEANサイバーセキュリティ協力等）

オープンデータ、ビッグデータ

○公共データの民間開放（オープンデータ）・ビッグデータの活用の推進
➢2015年度末には、他の先進国と同水準の公開内容を実現
➢IT総合戦略本部の下で、パーソナルデータの取扱いについて、制度見直し方針を年内に策定

2.「サイバーセキュリティ戦略」への反映

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅰ. 基本的な考え方

①情報の自由な流通の確保を基本原則とする
②管理や規制を過度に行うことなく、信頼できるサイバー空間の構築
③完璧主義から脱却し、リスク認識に基づく対応の強化（事故前提社会）
④産学官がそれぞれの役割を果たす動的防御連携の確立
⑤国際連携によるサイバー空間政策の推進

反映

Ⅱ.（1）産学官それぞれの役割による動的防御連携プロセスの確立（抄）

変化の激しい情勢に動的に適時適切に対応するためには、①モニタリング、②情勢判断、③意思決定、④行動というプロセスを有機的に連携させて繰り返し、それぞれのプロセスにおける機能の高度化を図りつつ、迅速かつ的確な意思決定を行う仕組みを構築することが必要である。

脚注3 Observe（モニタリング）、Orient（情勢判断）、Decide（意思決定）、Act（行動）を繰り返すことにより、迅速かつ的確な意思決定を行うという考え方。頭文字を取ってOODAループと呼ばれている。

反映

「サイバーセキュリティ戦略」

2. 基本的な方針

①情報の自由な流通の確保
②深刻化するリスクへの新たな対応
③リスクベースによる対応の強化
④社会的責務を踏まえた行動と共助

4.（1）推進体制等（抄）

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

脚注54 例えば、Observe（モニタリング）、Orient（情勢判断）、Decide（意思決定）、Act（行動）を繰り返すことにより、迅速かつ適格な意思決定を行う「動的防御プロセス連携」（OODAループ）

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅱ.(1) モニタリングにおけるインシデント認知機能の向上(抄)

「学」・「官」による技術の研究開発や制度の見直しなどによって、「産」によるインシデントの迅速な認知を下支えするような連携の枠組みを確立する。

特に、ISPなど事業者は、インシデントの認知機能を強化することなどを通じ、安心・安全なインターネット環境の整備に貢献する。

(短期的な対策)

- CCCの取組に加え、ウェブ型感染への対策として、マルウェアの感染元のような悪性サイト情報を蓄積するデータベースを構築する。また、認知機能の向上に向けて、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する。(新たなCCCの一環として実施。)
- 独立行政法人情報通信研究機構(NICT)において、潜在型マルウェアの挙動・検知など、サイバー攻撃の検知機能の向上に向けた技術の研究開発や実証実験を実施する。また、NICTの研究環境については、産学官の知見が共有されたサイバーセキュリティ技術に関する試験評価にも広く活用する。
- 総務省が推進するPRACTICEを活用したサイバー攻撃に関する情報共有などの国際連携について、対象国を米国やインドネシア等から欧州、ASEAN諸国に拡大し、インシデントの国際的な動向などを把握する。
- 新たなサイバー攻撃の出現に応じて、ISP等が自律的に情報セキュリティ上のインシデントを迅速に認知できるよう、技術的・制度的な観点から検討する。

反映

反映

「サイバーセキュリティ戦略」

3.(1)④サイバー空間の衛生(抄)

ネットワーク型のボットウイルス感染対策として、ISPの協力を得て実施された官民連携プロジェクトであるCCCでは、一般利用者に注意喚起等を行う取組が行われてきた。今後、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ISP等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する。

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

3.(3)②国際展開(抄)

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

予算施策

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

II.(1) モニタリングの高度化に資するサイバー攻撃の解析能力の向上（抄）

モニタリングの高度化に資するサイバー攻撃の解析能力の向上を図る。

具体的には、NICTを中心に、多様化した解析機能の連携を図り、我が国における解析能力の高度化を推進するとともに、高度情報セキュリティ人材を育成する。

（短期的な対策）

- 平成25年4月、NICT「サイバー攻撃対策総合研究センター」において、官民の英知を集めたオールジャパン体制での研究を開始する。具体的には、NICTは、潜在型マルウェアの高精度かつ迅速な検知に向けた技術開発など高度解析に向けた研究開発や実証実験を強化し、研究機能を有した高度な新たなサイバー攻撃にも対応可能な解析主体としての役割を発揮する。

（中期的な対策）

- 上記の研究開発や実証実験の成果を「産」におけるインシデントの認知に反映し、連携を強化する。
- 上記の研究開発や実証実験の強化を通じ、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。

反映

「サイバーセキュリティ戦略」

3.（2）②研究開発（抄）

我が国自らが最先端の研究開発を保持・向上することを目的に、研究機関等におけるサイバー攻撃の検知機能や高度解析等の向上に向けた技術の研究開発や実証実験を加速させる。

脚注102 例えば、NICTにおいて、解析能力等の向上に向けて、2013年4月、「CYREC（サイレック）」（Cybersecurity Research Center）として、オール・ジャパンの英知を結集したサイバーセキュリティ研究開発拠点を構築し、本格稼働。

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

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅱ.(1) 自律的な情勢判断の促進（抄）

既存の様々な監視機能の横断的な連携によって集積・蓄積された観測データや解析データなどを提供することにより、個々人が自律的に情勢判断を行うことが可能となるような仕組みを構築する。

（短期的な対策）

- 「サイバー攻撃解析協議会」で蓄積された情報などを踏まえ、サイバー攻撃の防御モデルを検討し、演習用テストベッドを利用した官民のLAN管理者等の参加による実践的な防御演習を実施する。
- 上記実践演習の対象やその手法の提供等については、官庁・大企業にとどまらず、地方公共団体や中小企業まで拡大する。

（中期的な対策）

- 「サイバー攻撃解析協議会」について、構成団体それぞれの監視機能の有機的な連携によって観測データ等の監視情報の蓄積を図り、サイバー攻撃の動向に関する我が国の総合的な情報提供機関としての位置づけを図る。
- 上記の情報などを踏まえつつ、防御モデルの検討・実践演習の実施というサイクルを回し、ICT利用者全般の防御能力の向上を推進する。
- 各主体における自律的な情勢判断の促進に資するよう、ICTに関する資格制度について検討する。

反映

反映

「サイバーセキュリティ戦略」

3.（1）③企業・研究機関等における対策（抄）

サイバー攻撃の防御モデルの検討及び演習用テストベッドを利用した実践的な防御演習について、大企業のみならず中小企業等も対象とすることにより、サイバー攻撃への対応能力等の向上を図る。

3.（1）④サイバー空間の衛生（抄）

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

予算施策

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」		「サイバーセキュリティ戦略」
II.(1) 情報共有の円滑化に向けた仕組みの検討 サイバー攻撃に関する官民の情報共有の円滑化に向けて、内閣官房情報セキュリティセンターなどと連携し、公的機関が実施する届出制度の整理や事業者のインセンティブ（義務づけと免責の仕組みなど）、協調対処のあり方などについて検討する。	反映	**4.（1）推進体制等（抄）** 政府機関や重要インフラ事業者等の関係機関間の有機的な連携のための基盤として、サイバー攻撃に関するインシデント情報等の共有を促進することが必要である。このため、攻撃者等に対して秘密とすべき情報について、既存の仕組みも活用しつつ、共有する目的、共有される情報等の内容や共有する者の範囲等に応じた秘密の保持のための枠組みを整備する。
II.(2) 個人利用者に対して自律的な対応を促すような意識啓発（抄） 「情報セキュリティ月間」における普及啓発活動について更なる充実を図るとともに、ホームページ等による一般的な普及啓発にとどまらず、ISP等による注意喚起等を通じて、個人がリスクを認識し、自律的な対応を実施するような仕組みを構築する。	反映	**3.（1）③企業・研究機関等における対策（抄）** 一般利用者等における認識の醸成を目的とする総合的・集中的な普及啓発については、毎年2月の「情報セキュリティ月間」及び毎年10月の「情報セキュリティ国際キャンペーン」として関連行事等を開催している。今後、政府一体としての取組を行うとともに、その一環としてサイバー空間の衛生の確保を国民運動とするため、例えば、放送大学における「情報コース」等の情報セキュリティの基礎となるソフトウェア教育との連携や、功労者の表彰等を行う「サイバー衛生の日（サイバー・クリーン・デー）」（仮称）の新設など一般利用者等の認識の更なる醸成を図るための取組を行う。 また、日常からの効果的な普及啓発について、ソフトウェア等の脆弱性関連情報の収集や各種インターネット定点観測システムの連携等を推進するとともに、我が国におけるサイバー空間の脆弱度やマルウェア感染度等の全体傾向等の可視化や、一般利用者等への的確な発信等を行う仕組みについて検討する。
	反映	**3.（2）④リテラシー向上（抄）** スマートフォンへの移行に伴い、その利用率が大幅に拡大しているSNS等、スマートフォンの利用に関する効果的な対策等について、関係事業者等と協力しその確保を図る。さらに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する。

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅱ.(2) 中小企業における情報セキュリティ対策の底上げ（抄）

中小企業に自ら情報セキュリティ対策を実施するインセンティブを持たせるため、情報セキュリティ対策の低コスト化に向けた仕組みなどを構築する。

また、セミナー開催など一般的な意識啓発にとどまらず、クラウド型の情報セキュリティへの移行や「中度」の人材育成など、最低限の情報セキュリティを確保するためのツールを「パッケージ」で提供し、社会全体として情報セキュリティ上のリスクを軽減するようなシステム作りを促進する。

反映

Ⅱ.(3) 政府機関・地方公共団体における情報セキュリティ対策の強化

政府は民間企業などよりも高度な情報セキュリティ対策を率先して実施する。

（短期的な対策）
- 各府省庁のCISO機能やCSIRT機能の充実に取り組む。
- 各府省庁の情報共有体制の充実に取り組む。
- 政府共通プラットフォームの整備の推進により、政府情報システム全体のセキュリティ対策の強化を進める。
- 政府職員の訓練の充実に取り組む。

（中期的な対策）
- 新たな情報セキュリティ上の脅威に迅速に対応できる体制整備について検討するとともに、国際連携の強化を図る

反映

「サイバーセキュリティ戦略」

3.（1）③企業・研究機関等における対策（抄）

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

3.（1）①政府機関等における対策

政府横断的な情報システムの対策強化に取り組む。具体的には、政府共通プラットフォームによる政府情報システムのクラウド化等を通じて、サイバー攻撃や大規模災害に強い政府情報システム基盤を構築する。

インシデント発生時におけるGSOC、CYMATと各府省庁等のCSIRTの間の連携を強化し、インシデント情報の速やかな共有と政府一体となった即応体制を構築する。

政府における平常時及び緊急時の対応力を強化するとともに、国際連携を促進するため、人材の確保・育成に取り組むことが必要である。

迅速かつ的確な対処を行うため、各府省等のCSIRT要員及びCYMAT要員の育成等を強化する。

予算施策

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

II.(4) 重要インフラ分野における情報セキュリティ分野対策の強化

重要インフラ事業者間の連携強化、官民の情報共有体制の充実など、重要インフラに対する情報セキュリティ上の脅威を軽減する枠組み作りを構築する。特に、新たなサイバー攻撃への対処という観点から、重要インフラ事業者と情報セキュリティの専門家との連携強化が急務であり、これは我が国の安全保障上の観点からも重要な課題である。また、安全な国民生活を実現する観点から、最低限確保すべき分野を特定し、対策を講じることが必要である。

(短期的な対策)

- 安全な国民生活を実現する観点から、スマートグリッド、スマート家電や自動車など新たな分野について、情報セキュリティの確保に向けた具体的な対策を検討する。

(中期的な対策)

- 重要インフラ事業者間の相互依存性が高まる中、重要インフラ事業者間の連携強化、官民の情報共有体制の充実など、重要インフラに対する情報セキュリティ上の脅威を軽減する枠組みを構築する。

反映

「サイバーセキュリティ戦略」

3.(1)②重要インフラ事業者等における対策

障害情報及び攻撃・脅威・脆弱性等に関する情報については、引き続き重要インフラ事業者等及びCEPTOARとの間における情報共有を推進するとともに、業種間での情報共有が難しい標的型攻撃に関する情報については、秘密保持契約に基づく情報共有体制を深化・拡充する。

重要インフラ事業者等、サイバー空間関連事業者及び関係CSIRTの間で、民間組織間の信頼関係を前提に、サイバー演習等の実施を促進しサイバー攻撃に対する連携対応能力の強化を図る。

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

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅲ.(1) グローバルなインターネット環境の安全の確保

日本の直接投資が活発なASEAN諸国など諸外国における安全な情報セキュリティ環境の水準を高めるため、技術的及び制度的な観点から多様な国際連携を推進する。また、国際連携を推進する前提として、日本国内の制度整備を着実に実施する。

(短期的な対策)

- サイバー攻撃に関する情報共有などの国際連携について、対象国を米国やインドネシア等から欧州、ASEAN諸国に拡大し、サイバー攻撃の発生を予知し、即応を可能とする技術の研究開発・実証実験を実施する。
- 官民連携によるウェブ型感染対策である新たなCCCを日本のベストプラクティスとして国際展開するとともに、諸外国と共同して実施する。
- 国内のみならず海外のISPなど事業者間による机上演習を実施する。
- 我が国における暗号評価プロジェクトの成果などを海外に展開する。
- 本年9月に開催予定の日ASEANサイバーセキュリティ協力に関する閣僚政策会議等を通じて、ASEAN諸国の情報セキュリティ環境の高度化を支援する。

(中期的な対策)

- 国内外のISPなど事業者がインシデント対応などで連携できる体制を構築する。
- 国際連合等の場を活用し、我が国の情報セキュリティ確保に向けた取組や成功事例を積極的に発信するとともに、ASEAN諸国のみならず、新興・途上国に対する国際協力を強化する。

反映

「サイバーセキュリティ戦略」

3.(2)①国際展開(抄)

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

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

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

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

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅲ.(2) 日本企業のグローバル展開への貢献

内閣官房情報セキュリティセンターや外務省、経済産業省など省庁の枠を超えて連携し、不合理な規制の撤廃に向けて、制度や技術的ノウハウなど総合的なパッケージ施策の展開を提案するなど、日本企業が国際進出可能な環境の整備に貢献する。

また、動的防御プロセス連携の確立とそれを支える研究開発の促進によって、創意と工夫に満ちた情報セキュリティ技術を生み出し、国内の情報セキュリティ産業を育成するとともに、世界に展開する。

(短期的な対策)

- 日ASEANサイバーセキュリティ協力閣僚会議やOECDなど国際機関の会議など多国間や二国間の会合において、検閲など不合理な規制の撤廃に関し、諸外国と協調に向け関係を醸成する。
- 悪性サイト等の検知機能の高度化など日本の研究開発の成果を活かしたベストプラクティスを国内の情報セキュリティ産業と連携しながら国際展開し、これらの海外進出を支援する。

(中期的な対策)

- 関係国と連携して、情報セキュリティの名の下で行われる諸外国の検閲など不合理な規制の撤廃に取り組む。

反映

反映

「サイバーセキュリティ戦略」

3.(2)①外交(抄)

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

3.(2)②国際展開(抄)

新興国等に見られる、情報セキュリティの名を借りた輸入制限や国産品優遇措置などの規制に対しては、国際的な貿易ルールに整合するように求めていくと同時に、国内外における関連制度等の整合性の確保を図ることにより、日本企業の国際展開の促進を図る。

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅲ.(3) 国際的なサイバー空間の規範形成への主導的な取組

内閣官房情報セキュリティセンターや外務省などと連携し、国際電気通信連合(ITU)にとどまらず、例えばサイバー犯罪の法規制など、これまで十分フォローできていなかったサイバー関係の国際会議に積極的に関与し、顔が見える外交を展開する。特に、スタンスの近い国々との連携強化に努め、先導的に国際的なサイバー空間の規範形成をリードする。また、情報セキュリティ分野とプライバシー分野との連携を図る。

(短期的な対策)

- 内閣官房情報セキュリティセンターや外務省などと連携し、当面予定されているサイバー空間に関するソウル会議やこれまで十分フォローできていなかったサイバー関係の国際会議において、顔が見える外交を展開する。

(中期的な対策)

- 内閣官房情報セキュリティセンターや外務省などと連携し、対外的に情報発信が強化できる体制について検討を行う。
- 日本と同様の考え方を有する国々と連携し、国際的な議論をリードするとともに、ネット規制・政府管理化に傾倒しがちな新興・途上国に対しても、理解が得られるよう努力し、協調路線の拡大を図る。

反映

「サイバーセキュリティ戦略」

3.(2)①外交(抄)

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

これまで二国間協議・対話を行ってきた国及び機関等との協議・対話を継続しつつ、その他の国等との協議・対話又は意見交換も拡大させていく。また、国連における関連会議やARFなどの地域的枠組を始めとした多国間協議・会合等、加えて、政府機関だけでなくマルチステークホルダーが参画するサイバーセキュリティ関連の各種会議やグローバルなコミュニティ等においても「顔の見える」形で積極的に参画する。

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」		「サイバーセキュリティ戦略」
V.(1) 情報セキュリティ産業の振興 国内の情報セキュリティ産業の育成の観点から、研究開発や人材育成などに取り組み、これらのグローバル展開を支援する。 また、ICT利活用の普及を踏まえ、交通、医療、流通などあらゆる分野の社会経済活動において情報セキュリティの確保が重要な課題となる。情報セキュリティ上の課題について幅広く指摘することにより、各分野の情報セキュリティ対策が向上し、広義の情報セキュリティ産業の振興に寄与していく。	反映	**3.(2)①産業活性化（抄）** 新たな技術が採用された製品等の調達を政府が積極的に行うことにより、民間企業等における製品開発、実用化や海外市場の獲得等を促進するとともに、ベンチャー企業を育成する。また、情報セキュリティ分野でグローバル競争に対等に伍していくことのできる強い企業を国内に有していく観点から、産業や組織の壁を超えた連携の促進や、潜在力を持つ企業のグローバル展開の支援を図る。
V.(2) 情報セキュリティ投資促進税制の検討 情報セキュリティ対策の低コスト化を図る観点から、民間企業の情報セキュリティ対策の促進を図るための情報セキュリティ投資促進税制について検討を行う。その際、情報セキュリティ投資に対する負担が割高となる中小企業に配慮することが必要である。	反映	**3.(1)③企業・研究機関等における対策（抄）** 情報セキュリティ対策に関する専門的な人材の確保や十分な投資等が困難となっている中小企業等について、サイバー攻撃に関するインシデントの認知機能等を強化するための環境整備を行うことが必要である。具体的には、中小企業に寄り添った情報提供・相談体制の整備、情報セキュリティ投資を促進する税制等のインセンティブの検討、情報セキュリティ向上のための利用しやすいガイドライン・ツールの整備、クラウド技術の活用等により情報セキュリティが確保された共同利用システムへの移行促進等を図る。

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅴ.(3) 情報セキュリティ研究開発等の強化（抄）

総合的な情報セキュリティ研究開発戦略を策定する。当面、NICTの「サイバー攻撃対策総合研究センター」における高度解析に向けた研究開発等の強化や新たなCCCの取組による個人利用者への注意喚起、サイバー攻撃の防御モデルの確立・実践演習の実施等を拡充する。

反映

「サイバーセキュリティ戦略」

3.（1）②企業・研究機関等における対策（抄）

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

反映

3.（1）②企業・研究機関等における対策（抄）

ネットワーク型のボットウイルス感染対策として、ISPの協力を得て実施された官民連携プロジェクトであるCCCでは、一般利用者に注意喚起等を行う取組が行われてきた。今後、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ISP等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する。

反映

3.（2）②研究開発（抄）

我が国自らが最先端の研究開発を保持・向上することを目的に、研究機関等におけるサイバー攻撃の検知機能や高度解析等の向上に向けた技術の研究開発や実証実験を加速させる。

「サイバーセキュリティ戦略」への主な反映状況

主な反映状況

「総務省における情報セキュリティ政策の推進に関する提言」

Ⅴ.(4) 情報セキュリティ人材の育成

情報セキュリティに関する研究開発等を通して研究機関等における高度情報セキュリティ人材の育成を促進する一方で、情報セキュリティ人材として求められるニーズの多様化に応じて、資格制度を含む人材育成のあり方について検討を行う。

反映

「サイバーセキュリティ戦略」

3.(2)③人材育成(抄)

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

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

３．その他の政府戦略への反映

その他の政府戦略における「情報セキュリティ政策」の位置付け①

「経済財政運営と改革の基本方針について」（平成25年6月14日 閣議決定）

第2章　強い日本、強い経済、豊かで安全・安心な生活の実現

5．長期的に持続可能な経済社会の基盤確保

（4）安全・安心な社会の実現等（消費者行政、治安・司法、防衛等）

（治安・司法・危機管理等）

さらに、ITSの活用等「第9次交通安全基本計画」に基づく取組、「サイバーセキュリティ戦略」に基づく取組、海洋の安全確保、危機管理の充実強化等を通じ国民の安全・安心の確保に取り組むとともに、都市部における地籍整備を推進する。宇宙インフラを安全保障・防災等に活用するため、衛星の整備・活用のほか、安全かつ安定した宇宙利用に資する取組を推進する。

「日本再興戦略 －JAPAN is BACK－」（平成25年6月14日 閣議決定）

第Ⅱ．－4．世界最高水準のIT社会の実現

⑤サイバーセキュリティ対策の推進

世界最高水準のIT社会にふさわしい、強靭で活力あるサイバー空間を構築するため、「サイバーセキュリティ戦略」を踏まえ、政府機関や重要インフラにおけるセキュリティ水準及び対処態勢の充実強化や国際戦略の推進等、サイバーセキュリティ対策を強力に展開する。

○重要インフラ分野におけるインシデント対策の強化

□ サイバー攻撃に対する重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲等について検討を進め、今年度中に、「情報セキュリティ政策会議」において、新たな行動計画を策定する。

○サイバーセキュリティに関する国際戦略の策定

□ 我が国と戦略的に強い結び付きのある国・地域との多角的パートナーシップの強化、我が国が強みを持つセキュリティ技術の国際展開等を政府一体となって加速させるため、今年度中に、「情報セキュリティ政策会議」において新たにサイバーセキュリティ国際戦略を策定するとともに、来年度中に制御システム等のセキュリティの国内での評価・認証を開始し、インフラの整備・輸出等を促進する。

その他の政府戦略における「情報セキュリティ政策」の位置付け②

「世界最先端IT国家創造宣言」（平成25年6月14日 閣議決定）

Ⅴ. 戦略の推進体制・推進施策

3. サイバーセキュリティ

サイバー攻撃が現実のものとなるなどサイバー空間を取り巻くリスクが深刻化し、我が国の安全保障・危機管理に影響を及ぼすとともに、国際的な競争力を揺るがし、国民に多大な不安をもたらすおそれが生じている。

このような中、「世界最高水準のIT社会」の実現を目指す我が国において、サイバーセキュリティの強化は、国家の安全保障・危機管理のみならず、IT・データ利活用の促進等を通じた我が国の産業競争力強化等のためにも不可欠なものである。

したがって、サイバーセキュリティについては、「サイバーセキュリティ戦略」（平成25年6月10日　情報セキュリティ政策会議決定）に基づき、具体的な施策を推進することを通じて、世界を率先する強靭で活力あるサイバー空間を構築することにより「サイバーセキュリティ立国」を実現する。

4. 参考

（参考）「サイバーセキュリティ戦略」の概要①

基本的な方針

(1) 目指すべき社会像：「サイバーセキュリティ立国」の実現

国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現

(2) 基本的な考え方

① 情報の自由な流通の確保
② 深刻化するリスクへの新たな対応
③ リスクベースによる対応の強化
④ 社会的責務を踏まえた行動と共助

(3) 各主体の役割

① 国	▸ サイバー空間の外交・防衛・犯罪対策、政府機関等における対策強化・対処態勢整備 等
② 重要インフラ事業者等	▸ 現行10分野の取組強化、新たな分野における必要な対策の実施 等 （10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）
③ 企業や教育・研究機関	▸ 情報共有等の集団的対策、産学連携による高度技術・人材の供給 等
④ 一般利用者や中小企業	▸ 「他者に迷惑かけない」認識醸成やリテラシー向上など自律的取組、情報共有 等
⑤ サイバー空間関連事業者	▸ 製品等の脆弱性への対応、インシデント認知・解析、国際競争力の強化 等

取組分野

2015年度までの3年間、以下に掲げる取組を実施。

(1)「強靭な」サイバー空間の構築

① 政府機関等における対策

- 政府共通プラットフォームによる情報システムのクラウド化、技術標準化等を通じ、攻撃等に強いシステム基盤構築。
- 大規模サイバー攻撃事態等を想定した対処訓練を毎年度実施するなど対処態勢を強化。

② 重要インフラ事業者等における対策

- 重要インフラ事業者等の攻撃情報等の情報共有を促進。

③ 企業・研究機関等における対策

- セキュリティ投資促進のためのインセンティブ検討等により、サイバー攻撃認知機能等を強化。
- 演習用テストベッドを利用した実践的な防御演習等により、企業等におけるサイバー攻撃への対応能力を向上。

（参考）「サイバーセキュリティ戦略」の概要②

（1）「強靭な」サイバー空間の構築 ［続き］

④ サイバー空間の衛生
- 悪性サイトにアクセスしようとする一般利用者に対するISP等による注意喚起等を行うための仕組みを構築。
- セキュリティ目的の通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方を検討。

⑤ サイバー空間の犯罪対策
- サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討。

⑥ サイバー空間の防衛

（2）「活力ある」サイバー空間の構築

① 産業活性化
- 我が国のサイバーセキュリティ産業の国際競争力の強化に向けた高度な技術開発や国際標準化の促進。

② 研究開発
- サイバー攻撃の検知や高度解析等の向上に向けた技術の研究開発等を加速させ、最先端の研究開発を保持・向上。
- 潜在型マルウェア等多様・高度化するサイバー攻撃に対し、有効な革新的技術を確立するため、先端技術を開発。

③ 人材育成
- 情報セキュリティ人材として求められるニーズの多様化に応じた資格等のあり方などについて検討。

④ リテラシー向上
- 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、利用等の判断を行う自ら行える仕組みを構築。

（3）「世界を率先する」サイバー空間の構築

① 外交
- 米国等との間で、サイバー領域での具体的対処の在り方、国際的なルール作りといった分野における議論を深化。
- 諸外国と連携してサイバー攻撃に関する情報収集ネットワークを構築し、攻撃の発生予知、即応等に関する研究開発を実施。

② 国際展開
- ASEAN等と連携し、国内における成功事例の紹介や共同プロジェクト、机上演習等を実施。

推進体制等

- NISCは、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組・機能強化
- 2015年度までの3年間を戦略の対象とし、年次計画の策定・評価等を実施
- 国際分野における総合的な対応を推進するため、サイバーセキュリティ国際戦略を策定

（参考）「総務省における情報セキュリティ政策の推進に関する提言」の概要（平成25年4月5日公表）

Ⅰ．情報の自由な流通の確保

人間の尊厳、自由、民主主義等の核心的な価値を推進するサイバー空間の構築による経済成長の促進。

Ⅱ．過度な規制によらない信頼できるサイバー空間の構築

イノベーションや経済成長を起こすサイバー空間の堅持。

Ⅲ．動的防御プロセス連携の確立

高度化・複雑化するサイバー攻撃に対応するためには、PDCAという一連のサイクルが終わる前に、常に、動的に、適時適切な意思決定を行うプロセスの構築が必要。

動的防御プロセス連携

それぞれのプロセスにおいて得られた知見を常時他のプロセスに反映

①モニタリング（検知・解析）（Observe）
- ◇継続的なモニタリングによるサイバー攻撃の検知
- ◇サイバー攻撃の目的・意図を判別するための情報収集

②情勢判断（Orient）
- ◇攻撃の目的・意図を識別した上で、自組織に対する影響を把握

③意思決定（Decide）
- ◇サイバー攻撃に対する措置に関する迅速かつ的確な意思決定

④行動（Act）
- ◇問題解決やリスク要因の排除の実施

総務省の取組

官民連携	悪性サイトの検知機能の強化	サイバー攻撃解析協議会による観測データ等の蓄積
国際連携	PRACTICE※1による諸外国とのサイバー攻撃情報の共有	
技術開発・人材育成	NICT「サイバー攻撃対策総合研究センター（CYREC※2）」による解析能力の向上	サイバー攻撃の防御モデルの確立・実践演習の実施※3

政府自身の防御体制の構築

- 政府情報システムの情報セキュリティ対策の強化。
- 職員訓練の充実。

※1 諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを国際的に構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験プロジェクト。

※2 Cybersecurity Research Center

※3 演習用テストベッドを利用した官民のLAN管理者等を対象に実践的な防御演習を実施。対象やその手法の提供等は、官庁・大企業にとどまらず、地方公共団体や中小企業に拡大。

Ⅳ．リスク認識に基づく対応の強化（事故前提社会）

自律的な対応を促す仕組みづくりの構築。

個人
- 通信事業者によるマルウェアの感染や悪性サイトへのアクセスに対する注意喚起等の実施。
- スマホのアプリについて、個人がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みの構築。

中小企業
- 情報セキュリティ投資促進税制等のインセンティブの検討。
- システムの共同利用など全体として低コストの情報セキュリティ対策の実現に向けた対策の推進。

Ⅴ．国際連携によるサイバー空間政策の推進

我が国の経済成長を見据えた戦略的な国際連携の推進。

グローバルなインターネット環境の安全の確保
- 共同プロジェクト推進等のASEAN諸国等との連携による情報セキュリティ環境の向上。

日本企業のグローバル展開への貢献
- 情報セキュリティの名の下で行われる過度な規制の撤廃に向けて省庁の枠を超えて連携。

国際的なサイバー空間の規範形成への主導的な取組
- 顔が見える外交を展開し、先導的に国際的なサイバー空間の規範形成をリード。