別紙３

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

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

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プロセス連携の確立
⑤ 国際連携によるサイバー空間政策の推進

Ⅱ．高度化する新たなサイバー攻撃への動的防御プロセス連携の確立

（1）産学官それぞれの役割による動的防御プロセス連携の確立

○モニタリングにおけるインシデント認知機能の向上
○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
○自律的な情勢判断の促進
○情報共有の円滑化に向けた仕組みの検討

（2）利用者に自律的な対応を促す仕組みづくり

○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の実施
○中小企業における情報セキュリティ対策の底上げ

（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

（4）重要インフラ分野における情報セキュリティ対策の強化

Ⅲ．我が国の経済成長を見据えた戦略的な国際連携の推進

（1）グローバルなインターネット環境の安全の確保
（2）日本企業のグローバル展開への貢献
（3）国際的なサイバー空間の規範形成への主導的な取組

Ⅳ．情報セキュリティの確保に向けた社会制度全般の最適化

Ⅴ．信頼できるサイバー空間を構築するための環境整備

（1）情報セキュリティ産業の振興
（2）情報セキュリティ投資促進税制の検討
（3）情報セキュリティ研究開発等の強化
（4）情報セキュリティ人材の育成
（5）パーソナルデータの利用・流通の促進

Ⅰ．基本的な考え方

インターネットは今やあらゆる社会経済活動を支える基盤であり、これによる経済成長や民主主義の実現などが期待されている。

このためには、まず、サイバー空間における情報の自由な流通の確保を、何よりも優先すべき基本原則として位置づけるべきである。なぜならば、過度な管理や規制[1]は、インターネットによる経済的・社会的便益を減殺し、結果としてインターネットによる経済成長を阻害する要因となる恐れがあるからである。換言すれば、情報の自由な流通の確保という目的を達成するための手段として情報セキュリティ対策を位置づけるべきであって、その逆であってはならない。インターネット規制の在り方については、政府だけではなく、企業やユーザーの市民も参画する形による対応（マルチステークホルダーアプローチ）が最善の方法である。

昨今、我が国の企業、個人、政府組織を狙ったサイバー攻撃が顕在化し、情報セキュリティ上のリスクが国民生活や経済活動にも影響を及ぼしており、これらに迅速かつ的確に対応することが求められている状況にある。

このため、情報セキュリティに係るリスクは常に存在すること、事前に全てを完全に防御すること（完璧主義）は重要であるが困難であることを認識した上で、リスクを考慮した社会意識、社会行動へ転換すること、また、このようなサイバー攻撃に迅速に対応できるよう、対処体制を抜本的に見直すことが必要となる。

さらに、国際的には、サイバー空間に関する規範形成の動きや国家安全保障の観点からの議論が活発化しており、我が国の経済成長を見据えた戦略的な国際連携を推進する必要がある。

以下、情報セキュリティ政策における5つの基本的な考え方を示す。

① 情報の自由な流通の確保を基本原則とする
- 人間の尊厳、自由、民主主義、平等、法の支配、基本的権利の尊重など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。

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
- 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。

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）
- 情報セキュリティに関するインシデントは必ず発生し、全てのサイバー攻撃を完璧に防ぐことは困難であるという認識の下での情報セキュリティ対策。

④ 産学官がそれぞれの役割を果たす動的防御プロセス連携の確立

1　2012 年 12 月、国際電気通信連合（ＩＴＵ）において、各国政府を法的に拘束する国際電気通信規則（ＩＴＲ）を改正する世界国際電気通信会議（ＷＣＩＴ）が開催され、インターネット規制のあり方が議論の焦点となった。通信内容の規制やインターネットへの国家関与の強化等を指向するアラブ、アフリカ、ロシア、中国等とこれらを最小限としたい日米欧等との間で、交渉が重ねられたが共通認識までは至らなかった。結果、規則は改正されたが、日米欧等 55 か国は署名に至っていない状況。

- 従来のPDCA[2]的アプローチを抜本的に見直し、新たな考え方に基づく対応の必要性の増大。
- （ⅰ）情報セキュリティ上の解析を通じたモニタリング、（ⅱ）情勢判断、（ⅲ）意思決定、（ⅳ）迅速な対処行動という動的防御プロセス連携に則って産学官がそれぞれの役割を果たす枠組みの確立。

⑤ 国際連携による<u>サイバー空間政策の推進</u>

- 国際的な規範形成の動きや新興国の発展、国家安全保障などを見据えたグローバルな視点からの政策の推進。
- ICT利活用による経済活動や持続的発展を支えるという視点とともに、世界に展開可能で我が国発の新産業創出、経済成長につなげていくという視点からの情報セキュリティ政策の立案。
- 非伝統的安全保障の考え方に基づく政策の検討。
- 世界最先端の情報通信基盤から得られる知見など含め、我が国のスタンスを積極的に対外発信し、国際的なサイバー空間の規範形成に関する議論をリード。

上記のような基本的な考え方に立ち、以下、総務省における情報セキュリティ政策の推進について提言を行うが、ここでの提言は、総務省だけでは推進することが困難な施策も含まれており、内閣官房情報セキュリティセンターの下、関係省庁が連携して取り組むことが求められる。

[2] Plan（計画）、Do（実行）、Check（確認）、Act（改善）を繰り返すことにより、業務を継続的に改善していくという考え方。

Ⅱ．高度化する新たなサイバー攻撃への動的防御プロセス連携の確立

技術革新に伴い高度化する新たなサイバー攻撃に対応するためには、従来の完璧主義から脱却し、リスク認識の考え方への転換が必要となる。

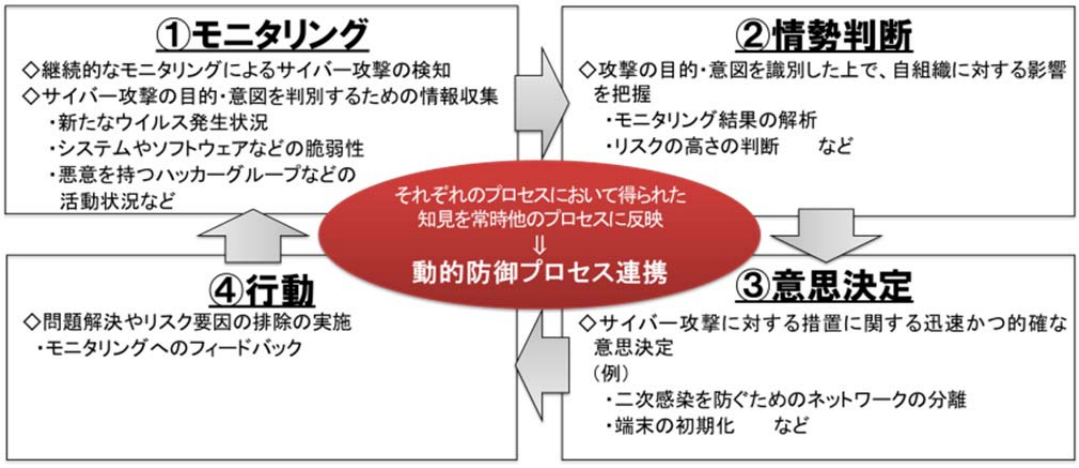
リスク認識の考え方に立ったうえで、産学官それぞれの役割による動的防御プロセス連携[3]の確立、また、ICTの利用者たる個人や中小企業に自律的な対応を促す仕組みづくりが急務である。

(1) 産学官それぞれの役割による動的防御プロセス連携の確立

インターネットを取り巻くリスクは、サイバー攻撃の高度化等に伴い、近年、急激に変化しており、従来のPDCAサイクルに基づく情報セキュリティ対策のままでは、有効な対策の立案・実施に遅れが生じ、効果が急低下することから、抜本的に対処体制を見直すことが喫緊の課題である。PDCAサイクルは確立した管理手法の一つであるが、計画を立ててからそれを一度実行したうえで初めて全体の改善を図る手法であるため、その意味ではサイクルが遅く、定型の判断では対処の難しい動的な状況には対応が難しい。

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。

動的防御プロセス連携のうち、意思決定及び迅速な対処行動については、これらの前提となるモニタリング及び情勢判断が適切に行われれば、各主体が自律的に対応を行うことが期待されることから、政府としては、モニタリング及び情勢判断の向上に資する対策を重点的に講じていくことが必要である。



図：動的防御プロセス連携

[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。

○モニタリングにおけるインシデント認知機能の向上

【問題意識】

技術革新に伴い高度化する新たなサイバー攻撃に有効に対応するためには、情報セキュリティ上のインシデントの認知がまず第一歩であり、そのための機能の確立が急務である。マルウェア感染の実態などを踏まえ、認知機能を向上することが必要である。

【解決の方向性】

「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。

（現状）

ネットワーク型感染が主流だった頃は、CCC（Cyber Clean Center）[4]の取組の下、ISP等はハニーポット等によりボットウイルスに感染したパソコンを検知し、利用者への注意喚起等を行い、世界トップクラスの低ボット感染率を実現した[5]。

最近はウェブ型感染に移行しており、新たな認知機能が必要となっている。

（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[6]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。**

4　我が国における、情報セキュリティ関係機関により実施されたサイバー攻撃の踏み台等になるボットウイルス撲滅に向けた取組。

5　2005 年の約 2~2.5%から 2011 年には約 0.6%に低下（CCC 調べ）。

6　総務省が平成 23 年度から実施している研究開発の一つ。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の研究開発及び実証実験を実施。現在、米国、インドネシア、タイ、マレーシア等と連携。（PRACTICE：Proactive Response Against Cyber-attacks Through International Collaborative Exchange）

（中期的な対策）

- 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。
- 認知機能の向上について、継続的な動的防御プロセス連携の実施を踏まえ、より効果的な施策を検討する。また、認知機能のリスク管理の観点からも、他府省庁や民間組織、外国組織で得られた知見、認知を積極的に活用する方策についても検討する。

○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

【問題意識】

有効な情報セキュリティ対策の確立には、サイバー攻撃の実態について解明するプロセスが必須となる。しかし、サイバー攻撃の巧妙化・複合化に伴い、これらの解析には従来のようなトラフィック量の観測だけでは足りず、高度な能力が必要となっている。また、個々の企業や個人がこのような能力を有しているわけではないので、中心となって解析を行い、情報セキュリティ対策の立案について広く貢献する主体が必要である。

【解決の方向性】

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。

（現状）

平成 24 年 11 月に、NICTにおいて、NICT内の情報セキュリティに関連する研究所の横断的な連携を強化するとともに、対外的な窓口を一元化している。

（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。
- 解析機能を有する多様な団体の連携の中で、NICTが中心となって高度解析に資する知見を提供し、我が国全体の高度情報セキュリティ人材の育成に貢献する。
- 諸外国との連携を促進し、解析能力の向上に取り組む。

○自律的な情勢判断の促進

【問題意識】

有効な情報セキュリティ対策の確立には、適時適切なリスクの監視と各主体における情勢判断が必須となる。しかし、サイバー攻撃の巧妙化・複合化はこれらを難しくしていることから、各主体が最新のデータに基づいて自律的な情勢判断を行うことが困難な状況である。

【解決の方向性】

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。

（現状）

平成 24 年7月に、総務省、経済産業省及び監視機能を有する関係団体によって構成される「サイバー攻撃解析協議会」が設置され、それぞれの監視機能について連携を進めている。

（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。

○情報共有の円滑化に向けた仕組みの検討

【問題意識】

サイバー攻撃に関する官民の情報共有については、情報共有ネットワーク構築による取組が推進されているが、営業秘密の保護・保持と情報公開の要請とのミスマッチにより、進んでいないのが現状である。一方で、サイバー攻撃の届出制度も複数存在し、届け出の利点も見えないことが、情報共有の障壁となっている。

【解決の方向性】

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。

（現状）

情報セキュリティ上のインシデントが生じた場合に届出を受理する公的な機関が複数存在している。

（短期的な対策）

- 現行のサイバー攻撃に関する届出制度について、共有される情報の範囲、届出による効果などの観点から整理する。
- 標的型メールの受信などサイバー攻撃の初期段階における情報や新たなマルウェアの発生に関する情報などの共有体制を構築する。
- ある主体で発生した事案について、他の主体への対策立案に貢献できるような情報共有の仕組み（例えばデータベースの構築など）について検討する。
- 官から民への情報提供について、官民連携の実効性を高める観点から、リアルタイム性や共有される情報の範囲などについて検討する。

（中期的な対策）

- 情報共有の円滑化に向けた制度的なあり方について具体的に検討する。
- 国際的な情報共有体制の構築について検討する。

(2) 利用者に自律的な対応を促す仕組みづくり

事故前提社会への転換のもとでは、ICTの利用者自らが責任をもって必要な情報セキュリティ対策を講じることが求められるような「自己責任」が原則となる。

しかし、個人や中小企業など、現在の高度化したサイバー攻撃に対して自助努力では対応が難しい主体に対しては、政府は、自律的に対応を行うような仕組み作りを重点的に講じていくことが必要である。

○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の実施

【問題意識】

昨今の報道などから、個人も情報セキュリティ上のリスクがあることは認識しているが、自分自身あるいは周囲で実際にどのようなリスクがあるのかという認識までには至っておらず、結果として、サイバー攻撃が発生した場合に迅速に対応できないなどの恐れがある。

【解決の方向性】

「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。

（現状）

ネットワーク型感染が主流だった頃は、CCCの取組の下、ISP等はハニーポット等によりボットウイルスに感染したパソコンを検知し、利用者に対して注意喚起等を行い、世界トップクラスの低ボット感染率を実現した。

最近はウェブ型感染に移行しており、新たな注意喚起型の対策が必要となっている。

また、スマートフォンについては、「スマートフォン情報セキュリティ3か条」や「スマートフォン　プライバシー　イニシアティブ」の策定など、啓発を推進している。

（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、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個人利用者に対して、ISP等によってデータベースを参照した注意喚起等を実施する新たなCCCを推進する。
- 情報セキュリティに関するサポーター育成活動を進めるSPREAD[7]と連携し、上記注意喚起等を受けた個人利用者をフォローする枠組みを構築する。
- 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を構築する。

7　セキュリティ対策推進協議会。IT 関連団体・企業により運営され、全国各地の NPO 団体や教育機関と協働して、地域のパソコンやインターネット利用者を支援する「サポーター」を育成している。

（中期的な対策）

- **新たなサイバー攻撃の出現に応じて、ISP等が自ら個人利用者に対して情報セキュリティ対策を実施することが可能となるよう、技術的・制度的な観点から検討する。**

○中小企業における情報セキュリティ対策の底上げ

【問題意識】

経済活動の基盤としてますますICTの利活用が進む中、ものづくりの原動力として知的財産を有する中小企業がサイバー攻撃の標的、もしくは踏み台となる可能性がある。さらに、アウトソーシングと非正規雇用が増大する中で、委託先となる中小企業がセキュリティホールとなる可能性があること、また、情報セキュリティは企業の利益と直接的にはつながりにくいことから、組織のトップが情報セキュリティ上のリスクに対してあまり理解はなく、結果として組織全体の対策に遅れが生じていることは、社会全体の脆弱性に繋がる恐れがある。

【解決の方向性】

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。

（現状）

中小企業にかかわらず、ICT利用者全般に対して、「国民のための情報セキュリティサイト」や様々なメディアを活用した普及啓発活動を展開している。

（短期的な対策）

- 中小企業が情報セキュリティ対策を行うインセンティブを検討する。
- 情報セキュリティ対策がビルドインされたクラウドサービスに関する周知啓発を広く実施する。
- 最低限の情報セキュリティ対策に関する知識を有し、対応が可能な「中度」の人材を育成する方策について検討する。
- 自動化できる部分の切分けやシステムの共同利用を図る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を推進する。
- IPv4とIPv6が共存するインターネット利用環境への変化に伴う情報セキュリティに係る課題の対策確立に向けた実証実験を実施し、結果をガイドラインの形でとりまとめ、中小企業を含む官民の組織に対して提供する。

（中期的な対策）

- サイバー攻撃の実態を踏まえた防御モデルを確立し、中小企業を含む官民の組織に対して提供する。

(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

【問題意識】

情報セキュリティ基本方針の策定、CISO[8]等連絡会議の開催、情報セキュリティに係る年次報告書の策定などをはじめ、政府機関は自らのシステムに対する情報セキュリティ対策に努めているが、情報セキュリティ上の脅威の高度化に十分対応できているとは言えない。また、サイバー攻撃が安全保障面における脅威になるとの指摘も多く、諸外国に比べて十分な対策が講じられているか検証する必要がある。

【解決の方向性】

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。

(現状)

政府においては情報セキュリティ基本方針の策定など、各府省庁においてはCSIRT[9]機能の整備などを実施している。

(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。**
- **政府情報システム管理データベースにより、脆弱性検知機能を提供する。**
- **政府職員の訓練の充実に取り組む。**
- **地方公共団体における情報セキュリティ対策の強化を進める。**
- **総務省のネットワークについて、研究成果の知見を活用するなどNICTとの連携について検討する。**

(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。**

---

8 Chief Information Security Officer 組織における最高情報セキュリティ責任者。

9 Computer Security Incident Response Team 情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊。

(4) 重要インフラ分野における情報セキュリティ対策の強化

【問題意識】

情報通信、金融、電力などの重要インフラ分野[10]は、国民生活と密接な関係があるので、サイバー攻撃を受けた場合、経済社会に大きな影響が生じ、ひいては我が国の安全保障上の脅威となる可能性がある。最近、制御系システムに対するサイバー攻撃なども高度化しており、新たな脅威に十分対応できているとは言えない。さらに、重要インフラの運営者と情報セキュリティに関するノウハウを有するシステムベンダとの連携がうまくいっていないケースが見られる。

また、スマートグリッド、スマート家電の普及や自動車のインターネット化などにより、新たな領域において情報セキュリティ上の脅威が生ずる可能性がある。

【解決の方向性】

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。

（現状）

国民生活や社会活動に重大な影響を及ぼす分野として、情報通信、金融、電力など10分野を重要インフラ分野として、安全基準等の整備やセプターカウンシル[11]の活動を中心とした情報共有体制の強化などを推進している。

（短期的な対策）

- **テレコム・アイザック推進会議[12]は、T-CEPTOAR[13]幹事団体として、セプタ**

---

10 「重要インフラの情報セキュリティ対策に係る第２次行動計画」（ＩＴ戦略本部情報セキュリティ政策会議　2009 年 2 月決定、2012 年 4 月改定）では、「重要インフラ」を他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状況に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものとしており、「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」及び「物流」の 10 分野としている。

11 2009 年 2 月に発足した、重要インフラ各分野のセプター（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情報共有・分析機能を行う体制。）により構成される共助活動・情報共有の場。

12 正式名称は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。国内の主要なＩＳＰにより構成され、情報セキュリティインシデント情報等を収集・分析し、業界内で共有することを目的としている。

13 IT 障害の未然防止、IT 障害の拡大防止・迅速な復旧、IT 障害の要因等の分析・検証による再発防止を図り、電気通信事業者のサービスの維持・復旧能力の向上に資するため、政府等から提供される情報を適切に電気通信事業者等の間で共有・分析することを

ーカウンシルの活動において、引き続き、先導的な役割を発揮するとともに、電気通信事業者におけるサイバー演習等の枠組みを他の重要インフラに広げるなど取組を強化する。

- 東日本大震災の教訓を踏まえた重要インフラ事業者による情報セキュリティの観点も加味した事業継続計画（BCP）等の充実を促進する。
- 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。
- 新たなサイバー攻撃に強靱な重要インフラを確保する観点から、最新の情報セキュリティ技術の迅速な導入など重要インフラの運営者とシステムベンダ等情報セキュリティの専門家との連携のあり方について検討する。
- 重要インフラの情報セキュリティに関する国際連携の枠組みを構築する。

目的に設置された電気通信分野のセプター。

Ⅲ．我が国の経済成長を見据えた戦略的な国際連携の推進

情報の自由な流通を基本原則として、過度な規制のない信頼できるサイバー空間を国際連携によって構築することが必要である。

情報セキュリティの名の下で行われる検閲など不合理な規制に対しては、日本企業のグローバル展開に向け、省庁の枠を超えた連携により、国際機関等を通じて日本のスタンスを発信できる仕組み作りを講じることが必須である。

我が国の経済成長を促進する観点から、日本の直接投資が活発なASEAN諸国を中心に、ICT基盤の脆弱性を減らすための多様な国際協力を推進することが必要である。特に、インターネットやモバイルの短期間で急速な普及が予想されるアフリカ諸国等に対する情報セキュリティ分野における国際協力を推進していく必要がある。

(1)グローバルなインターネット環境の安全の確保

【問題意識】

海外に進出している日本企業だけではなく、海外の企業も安全なICT基盤の下で事業展開ができるよう、グローバルなインターネット環境の安全を確保することが必要である。また、これは、日本国内における経済活動の確保からも重要である。

【解決の方向性】

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。

（現状）

米国やインドネシア、タイ、マレーシア等とサイバー攻撃に関する情報共有を通じた国際連携を推進している。

（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。
- グローバルな迷惑メールの削減に向けて、制度的・技術的な迷惑メール対策のベストプラクティスの共有などを行う対象国を拡大する。
- 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。

- **APCERT[14]など既存の取組との連携を強化し、具体的な対策の実現に向けた国際展開を前進させる。**

（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。**

14 Asia Pacific Computer Emergency Response Team　アジア太平洋コンピュータ緊急対応チーム。アジア太平洋地域の CSIRT の連携を促進・サポートする目的で、2003 年 2 月に発足。

(2) 日本企業のグローバル展開への貢献

【問題意識】

一部の諸外国においては、情報セキュリティの名の下で行われる検閲など不合理な規制が散見されるようになっており、このような規制は、日本企業が国際進出を図るうえで足かせとなっている。

また、国内の情報セキュリティ産業の育成の観点から、情報セキュリティ産業のグローバル展開を支援することが必要である。

【解決の方向性】

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。

（現状）

二国間の会談において、日本企業のグローバル展開の支障となる相手国の規制について、撤廃を求めている。

CCCはベストプラクティスとして諸外国から高い評価を受け、類似の取組が国際的に実施されているが、日本の情報セキュリティ産業との結びつきは希薄である。

（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。

(3)国際的なサイバー空間の規範形成への主導的な取組

【問題意識】

新興・途上国でのネット規制・政府管理化の動きに対して、米国等から国境を越える自由な流通の確保を求める動きが展開されており、国際的にサイバー空間（インターネット政策）の国際規範に関する議論が活発化している。特に、新興・途上国は、あらゆる国際会議の場を活用してネット規制・政府管理化の議論を推進してきており、これまでに日本が積極的に関与してこなかった国際会議であっても、当該議論が行われる場合には、幅広く対応していく必要がある。

【解決の方向性】

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。

（現状）

日本は、「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歩」に関する政府専門家会合（国連サイバーGGE）等の国連関連会合やWCITをはじめとするITUの会合、ロンドン及びブダペスト国際サイバー会議等を中心に、積極的に対応しているが、必ずしも全ての関連会合について十分にフォローできているわけではない。

（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。

Ⅳ. 情報セキュリティの確保に向けた社会制度全般の最適化

【問題意識】

サイバー攻撃が常に発生するということを前提とした強靭な社会システムとなっていない。ICT利活用の発達により、各主体の活動について相互依存性が高まっていることから、社会制度全般を俯瞰し、情報セキュリティの確保に対して支障となっている制度の改善の必要性がある場合に、従来の制度を是正し、情報セキュリティの確保に向けて最適化していく機能が必要である。

【解決の方向性】

内閣官房情報セキュリティセンターなどと連携し、ICT利活用の広がりを踏まえた社会制度全般の見直しを行う。

（現状）

社会制度全般に関して、情報セキュリティの確保に向けて最適化していく機能が確立しているとは言えない。

（短期的な対策）

- **内閣官房情報セキュリティセンターや関係省庁と連携し、ICT利活用の広がりを踏まえ、どのような課題があるか検討を行う。**

（中期的な対策）

- **情報セキュリティに配慮した措置を講ずることを意識した「Security by Design[15]」の社会システムの構築について検討を行う。**
- **国民の情報ネットワークの安心・安全な利用に資する思考及び行動様式である「情報セキュリティ文化[16]」の定着を図る。**
- **情報セキュリティの確保に向けて社会制度全般を最適化していく仕組みづくりについて検討を行う。**

15　プライバシー分野では、パーソナルデータを利用する者は、商品開発時などそのビジネスサイクルの全般にわたって、プライバシーの保護をデザインとしてあらかじめ組み込んでおくこととする「Privacy by Design」という考え方がある。このような考え方と同様に、社会システム全般にわたって、情報セキュリティの確保への配慮をあらかじめ組み込んでいくような考え方を「Security by Design」とここでは呼ぶ。

16　「情報セキュリティ普及・啓発プログラム」（情報セキュリティ政策会議　2011 年 7 月 8 日策定）13 ページ参照。

Ⅴ．信頼できるサイバー空間を構築するための環境整備

(1) 情報セキュリティ産業の振興

【問題意識】

我が国の情報セキュリティレベルの向上を図るためには、その基盤となる情報セキュリティ産業の振興が不可欠である。一方で、現状は外資系の情報セキュリティ産業が多い。

【解決の方向性】

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。

(2) 情報セキュリティ投資促進税制の検討

【問題意識】

情報セキュリティ対策には、投資コストの問題がある一方で、情報セキュリティは企業の利益と直接的にはつながりにくいことから、結果として組織全体の対策に遅れが生じている。

【解決の方向性】

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。

(3) 情報セキュリティ研究開発等の強化

【問題意識】

高度化・複雑化するサイバー攻撃を防御するためには、我が国自らが最先端の研究開発能力を保持・向上することが極めて重要となる。また、リスク認識に基づく利用者による自律的な対応を促す実証など効果的な施策の展開に努めていくことが必要である。

【解決の方向性】

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。

(4) 情報セキュリティ人材の育成

【問題意識】

情報セキュリティの脅威が社会的な問題となっているにもかかわらず、情報セキュリティに関する人材が十分育成されているとは言えず、不足している状況にある。また、現行の情報セキュリティ関連の資格は、各主体が適切な情報セキュリティ対策を講ずるためのニーズに適合していない面もある。

【解決の方向性】

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。

(5) パーソナルデータの利用・流通の促進

【問題意識】

ICTの普及発達により、ライフログなど多種多様なパーソナルデータがネットワークを流通する中、このような情報の集積・利用に対しては、プライバシー保護に関する不安が生じている一方で、これによる新ビジネスの創出や国民の利便性の向上などが期待されている。また、クラウドサービスなどICTの普及発達により、国境を越えた情報の流通が極めて容易になっており、国際的な調和の取れた、自由な情報の流通とプライバシー保護などの双方を確保する必要性が高まっている。

【解決の方向性】

プライバシー保護などに配慮したパーソナルデータのネットワーク上での利用・流通の促進に向けた方策について検討を行う。

本検討は、現在、総務省「パーソナルデータの利用・流通に関する研究会」において議論されていることから、必要に応じて、「情報セキュリティ　アドバイザリーボード」から、問題意識や解決の方向性について問題提起を行う。