「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」について

別紙2

◇　総務省では、有識者から助言を得ることを目的として、**「情報セキュリティ　アドバイザリーボード」**（座長：山口　英　奈良先端科学技術大学院大学教授）を平成25年3月から開催。

◇　本年4月、高度化・複雑化するサイバー攻撃など情報セキュリティを取り巻く環境の変化を踏まえ、**「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」**を取りまとめ。

提言における基本的な考え方

以下の５つの基本的な考え方に立ち、総務省は、内閣官房情報セキュリティセンター等と連携しつつ、情報セキュリティ政策に取り組むことが求められる。

① 情報の自由な流通の確保

人間の尊厳、自由、民主主義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 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。

※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

③ リスク認識に基づく対応の強化（事故前提社会）

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の実施。

④ 動的防御プロセス連携の確立

PDCAというサイクルにとらわれることなく、常に、動的に、適時適切な意思決定を行う「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

我が国の経済成長を見据えた戦略的な国際連携の推進。

提言のポイント

動的防御プロセス連携の確立

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。

リスク認識に基づく対応の強化（事故前提社会）

個人や中小企業に対して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。

国際連携によるサイバー空間政策の推進

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。