資料2

「情報セキュリティ アドバイザリーボード ITSセキュリティ検討グループ」について

事務局

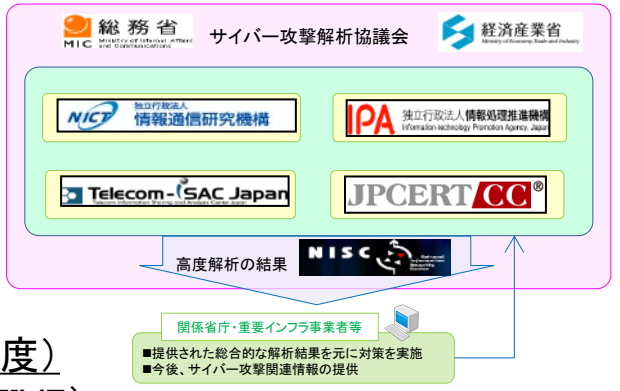
総務省の情報セキュリティ政策の概要

1. 安心なネットワーク環境の整備

①事業者との情報共有
・テレコム・アイザック推進会議等の所管事業者や(独)情報通信研究機構と情報共有し、被害の拡大防止等に寄与。

②サイバー攻撃対処に向けた官民連携の強化
・経済産業省及び関連4団体と、各機関が保有する情報を高度解析し、サイバー攻撃の実態等を把握(サイバー攻撃解析協議会)。

③ICT環境の変化に応じた情報セキュリティ対応方策の推進事業(平成25～29年度)
・ 国民のウイルス感染被害予防に資する研究開発・実証実験等を実施。(ACTIVE)



2. 技術開発の推進

①サイバー攻撃解析・防御モデル実践演習(平成24～29年度)
・サイバー攻撃への防御モデルの検討を行うとともに、官民参加型の実践的な防御演習を実施。(CYDER)

②国際連携によるサイバー攻撃予知・即応技術の研究開発(平成23～27年度)
・諸外国と連携して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を実施。(PRACTICE)

3. 利用者意識の向上

・「国民のための情報セキュリティサイト」による情報提供、セミナー開催による周知啓発活動。
・スマートフォン、無線LAN等の情報セキュリティに関する様々なメディアを活用した周知啓発活動

4. 国際連携の推進

・米国、ASEAN等の海外諸国と情報セキュリティ対策に関する取組を共有し、国際的な連携を推進。

5. パーソナルデータの利用・流通の促進

・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するため研究会を開催。

情報セキュリティ アドバイザリーボード

情報通信分野における官民において、時々刻々と変化する情報セキュリティ上の課題に対して効果的な対策や、日本の経済成長に繋がるような有効な施策が講じられるよう、**有識者から助言を得ることを目的として設置**する。

「情報セキュリティ アドバイザリーボード」の任務

（１）情報セキュリティ対策の在り方への助言

情報セキュリティの推進にあたり、日本の経済成長への貢献も視野に入れつつ、情報通信分野に携わる関係者において短期的及び中長期的に講ずべき対策や既存の取組の改善などの方向性について、幅広い観点から助言を行う。

（例）・ 官民連携や国際連携の在り方
・ 情報セキュリティに係る研究開発の方向性
・ DDoS攻撃や情報窃取など情報セキュリティに係るインシデント等への即応の在り方

（２）その他

情報セキュリティに係る諸問題への対応について、必要に応じて、提言をとりまとめる。

情報セキュリティ アドバイザリーボード

【構成員】（敬称略）

（座長）	山口　英	奈良先端科学技術大学院大学　教授
（座長代理）	林　紘一郎	情報セキュリティ大学院大学　前学長・教授
	飯塚　久夫	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　会長
	岡村　久道	国立情報学研究所客員教授・弁護士
	藤沢　久美	シンクタンク・ソフィアバンク　副代表
（顧問）	小野寺　正	KDDI株式会社　代表取締役会長

※政府の「情報セキュリティ政策会議」のメンバー

ワーキンググループ　【構成員】技術系や法律系などの有識者、電気通信事業者等

スケジュール　平成25年３月から随時開催。

「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

◇　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。

◇　平成25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
- 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。

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

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。

ITSセキュリティ検討グループにおける主な検討事項（案）

既存のガイドライン

■ 運転支援通信システムに関する運用管理ガイドライン（RC-008）

（平成23年4月27日ITS情報通信システム推進会議策定）

- 運転支援通信システムの実用化・運用・維持の際に必要となる運用事項について定めたもの。
- 情報セキュリティについては、各機器におけるセキュリティ情報の格納・更新・再設定・抹消の手続き等を規定。

■ 運転支援通信システムに関するセキュリティガイドライン（RC-009）

（平成23年4月27日ITS情報通信システム推進会議策定、平成24年4月25日改訂、平成25年11月25日改訂）

- 運転支援システムに対する脅威とリスクを分析し、脅威に対する対策方針について定めたもの。
- 情報セキュリティについては、車車間・路車間通信において、暗号技術を用いて発信元の真正性確認やメッセージの完全性確認を行うとともに、通信区間を流れる情報の機密性の確保を可能にすべきこと等を規定。

既存のガイドラインを踏まえてより具体的な検討を行う

検討グループにおける検討事項

これまで策定されたガイドラインを踏まえて、以下の事項について検討

セキュリティ規格書

基本ポリシー

情報セキュリティ対策に対する根本的な考え方
（適用範囲と適用者、情報資産および脅威、体制と役割）

対策基準書

基本ポリシーで定められたセキュリティ確保のための対策基準
（技術面、運用面、管理面）

メーカは策定された対策基準書を参照し、
基準書の内容を実現するための設計書・運用手順書を作成

検討の流れ

対象の定義　：　システムのモデル化
↓
リスク分析　：　脅威の洗い出しとリスク評価
↓
基本ポリシー策定：　対策をおこなう脅威の抽出
↓
対策基準の策定　：　対策目標の策定

当面のスケジュール（案）

■ 当面においては検討が進んでいる車車間・路車間通信における安全運転支援システムにおける情報セキュリティについて具体化を行い、平成26年4月を目途に中間的な取りまとめ（ガイドラインの策定）を行うこととする。その後、実証実験の結果を踏まえ、ガイドラインの改良などを行っていく。

平成26年　2月				3月				4月				5月			
1W	2W	3W	4W	1W	2W	3W	4W	1W	2W	3W	4W	1W	2W	3W	4W
		▲ 第1回 ・設立趣旨の確認 ・700MHz帯安全運転支援システムの説明 ・今後の進め方　等			▲ 第2回 ・セキュリティ方式の検討　等			▲ 第3回 ・セキュリティ方式の評価まとめ ・セキュリティ運用管理の評価　等				▲ 第4回 ・中間取りまとめ			
												取りまとめられた部分について、実用化に向けた実証を行うとともに、議論の対象を拡大し、引き続き検討を実施。			