「重要インフラのサイバーテロ対策に係る特別行動計画」のフォローアップ等について

<趣旨>

「重要インフラのサイバーテロ対策に係る特別行動計画」（平成12年12月15日 情報セキュリティ対策推進会議。以下「特別行動計画」という。）策定後の諸情勢の変化を踏まえ、各重要インフラ分野における特別行動計画への取組状況等についてのフォローアップを進めるとともに、それらの取組強化に向けた検討を行うこととする。

Ⅰ 官民における取組みの進捗状況等

特別行動計画に示された官民において取り組むべき各事項について、主な施策の実施状況は以下のとおりである。

1 被害の予防（セキュリティ水準の向上）

(1) 民間重要インフラ分野等のセキュリティ水準の向上

・ 金融庁では、金融検査マニュアルに基づく定期的な検査において、情報セキュリティポリシーの策定等についてチェックを実施。

・ 総務省では、平成13年3月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定し、地方公共団体に提示したほか、「情報通信ネットワーク安全・信頼性基準」（総務省告示）により情報通信分野における「情報セキュリティポリシーの策定のための指針」を規定。

・ 電力分野においては、事業者団体にて「電力におけるサイバーテロ対策危機管理ガイドライン」を作成。

・ その他、各所管省庁は事業者団体等における現状調査や行政上の指導・監督等を通じて、民間重要インフラ事業者等のセキュリティ水準向上について指導。

(2) 電子政府の構築に向けたセキュリティ水準の向上

・ 内閣官房の専門調査チームは、各省庁における情報セキュリティポリシーの策定状況のほか、サイバーテロ対策一般に関する問題点等について、昨年5月にヒアリング及び意見交換を実施。

・ 昨年10月、「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日 情報セキュリティ対策推進会議。以下「アクションプラン」という。）を策定。これに基づき、内閣官房は 2002 年夏を目途に各省庁の情報セキュリティポリシーについて再評価等を行うほか、これを受けて各省庁ではポリシーの見直しを実施予定。

・ 総務省及び経済産業省では、電子政府のための暗号技術評価を実施。

2 官民の連絡・連携体制の確立・強化

昨年10月にサイバーテロ対策に関する官民の連絡・連携体制の運用に関する基本的な考え方として、「サイバーテロ対策に係る官民の連絡・連携体制について」（平成13年10月2日 情報セキュリティ専門調査会。以下「官民の連絡・連携体制」という。）を策定。

また、昨年末までに当該連絡･連携体制の運用に関し、連絡経路等の必要な具体的事項を関係者間において取りまとめ。

3　官民連携によるサイバー攻撃の検知と緊急対処

(1)サイバー攻撃の検知

・「官民の連絡･連携体制」において、情報共有の対象となる重要システム、サイバー攻撃等のほか、攻撃検知時の手順について規定。

・内閣官房は昨年中、関係省庁等から事案発生に関する情報収集を行うとともに、注意喚起等として２８件の情報を各省庁へ提供。

(2)緊急時対応計画の策定

・総務省では、「情報通信ネットワーク安全･信頼性基準」（総務省告示）により、各電気通信事業者が緊急時対応計画等を整備するにあたっての「危機管理計画策定のための指針」を規定。

・電力分野においては、各電力事業者における緊急時対応計画等に反映させるための「電力におけるサイバーテロ対策危機管理ガイドライン」を事業者団体にて作成。

(3) 緊急時における情報の連絡手順

・「官民の連絡･連携体制」に関して、連絡経路等の必要な具体的事項につき、内閣官房や重要インフラの所管省庁等関係者間において取りまとめ。

(4) 政府における緊急対処体制の強化

・アクションプランに基づき、内閣官房では電子政府等に対するサイバー攻撃などの事案が発生した場合又はそのおそれがある場合に、政府として取るべき措置や再発防止措置の実施に資するための緊急対応支援チームを平成１４年度に編成。

・警察庁では、サイバーテロの未然防止、発生時における被害の拡大防止ための監視･緊急対処体制として、機動的技術部隊（サイバーフォース）を創設。

・防衛庁では、自衛隊等の保有する情報システムに対する常時監視、システム監査、緊急事態対処等の機能を備えた体制の整備を推進。

・情報通信分野においては、総務省、電気通信事業者及び事業者団体との間にて、サイバー攻撃への対応も含めた情報セキュリティ対策のための連携体制を構築。

・電力、ガス分野においては、経済産業省、民間重要インフラ事業者等及びそれらの事業者団体との間にて、サイバー攻撃への官民合同の対応体制を整備･強化。

・航空、鉄道分野においては、各事業者と国土交通省との間で、緊急事案発生時における初動対応体制を構築。

4　情報セキュリティ基盤の構築

(1) 人材育成の推進

・警察庁及び防衛庁では、米国等の政府機関や情報セキュリティ関連団体などへ職員を派遣し、研修、情報交換等を実施。

・総務省では、昨年７月、電気通信事業法に基づく電気通信主任技術者試験に情報セキュリティに関する科目を追加。また、事業者団体が情報セキュリティ分野の人材育成を推進するための協議会を設立し、同年９月から資格認定講習を開始。

・経済産業省では、平成１３年度に情報セキュリティアドミニストレータ試験を創設したほか、

情報セキュリティ評価技術者及び情報セキュリティ設計技術者の育成事業を推進。

(2) 研究開発の推進

・ 防衛庁では、サイバー攻撃に対する対処手法の実証的研究及びコンピュータ・システム等の安全性確立のための運用ガイドラインに関する調査研究を推進。
・ 金融分野においては、財団法人金融情報システムセンターにてセキュリティポリシー、コンティンジェンシープランの策定・運用に関する研究会を平成13年に実施。
・ 総務省では、第3世代移動通信システムに関する情報セキュリティ上の対策等について研究会を開催し、昨年12月に報告書を取りまとめたほか、平成13年度からネットワークセキュリティ基盤技術の推進のための研究開発等を通信・放送機構において実施。
・ 経済産業省では、コンピュータウイルス、不正アクセス等により情報処理システムが受ける脅威の状況やそれに対する防御措置に関する技術開発を推進。

(3) 普及啓発の推進

・ 内閣官房では、平成13年度中に「情報提供システム」を整備し、情報セキュリティに関する知識の普及・啓発を目的とするインターネットWebページを立ち上げ。
・ 国家公安委員会、総務省及び経済産業省では、民間部門におけるセキュリティ意識を向上させるため、不正アクセス行為の発生状況等を公表。
・ 金融分野においては、財団法人金融情報システムセンターにより事業者を対象とした情報セキュリティに関する各種セミナーを開催。
・ 経済産業省では、コンピュータ・ウイルス等に対する被害と対策についてのセミナーを全国各地で実施。

(4) 法制度の整備

・ 法務省では、いわゆるサイバーテロを含めた各種のハイテク犯罪に対する罰則の整備、情報通信ネットワークに関する捜査手続について、適切な処罰を確保するための法整備を2005年までに行うため、諸外国の法制度調査及びハイテク犯罪に関する国内事例調査を実施。

5 国際連携

・ 内閣官房では、本年3月、関係省庁の参加を得て、米国の情報セキュリティ対策担当者との日米政府間討議を開催。
・ 警察庁、総務省、法務省、外務省及び経済産業省では、G8リヨングループハイテク犯罪サブグループに参加し、ハイテク犯罪からの重要インフラの防護について各国と情報交換。
・ 防衛庁では、平成12年度から米国防総省等との政策協議などを行うため、「IT フォーラム」等を開催。
・ 総務省では、国際電気通信連合電気通信標準化部門(ITU-T)における情報セキュリティに関する標準化活動を推進。
・ 経済産業省では、昨年9月に情報セキュリティに関するOECDワークショップを開催したほか、本年3月にはアジア太平洋地域における各国の CSIRT(Computer Security Incident Response Team)を集めた国際会議を開催。
・ 内閣官房、警察庁、総務省、外務省及び経済産業省等は、OECDにおける1992年情報システム・セキュリティ・ガイドラインの見直し作業に参加。

Ⅱ　特別行動計画における取組みの強化に向けた検討課題

民間重要インフラ事業者等の取組みの状況については、これを把握するための体制、枠組みが存しない分野もあるほか、これら取組みの実効性の確保方策について、必ずしもその受皿や方策が整っていない現状が存する。

これを踏まえ、民間重要インフラ事業者等の情報セキュリティ確保に関する取組みを一層促進するべく、以下の課題に関し、今後の方向性や具体策について重要インフラ分野ごとに検討を進めることとする。

なお医療分野については、今後のIT化の進展状況等を見極めつつ、重要インフラ分野の1つに位置付けることについて、検討を進めることとする。

【検討課題】

①重要インフラの情報システムに関する現状把握･検証

重要インフラの基幹をなす情報システムに関し、それぞれのシステム構成やそれらの外部ネットワークへの接続の有無･運用状況のほか、サイバー攻撃を受けた場合に想定される事態などにつき、各分野内での把握･検証等の方策を検討する。

②民間重要インフラ事業者等におけるサイバーテロ対策状況の把握

各事業者等の取組状況の把握等を行うための手法･体制等を検討する。

③民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

各事業者等における取組みを一層効果的なものとするため、以下に例示する観点等から、官民における実効性の確保方策を検討する。

[例]

- 既存の検査体制等の活用など指導･監督の在り方
- 情報セキュリティに関する専門家等も参加した官民合同の検討体制等の在り方
- 事業者団体等における実効性担保のための体制の在り方

④その他政府における検討事項

政府においては、①から③の検討状況を踏まえ、以下に例示する観点等から、サイバーテロ対策の一層の促進方策について、その必要性を含め検討する。

[例]

- 重要インフラにおける情報セキュリティ確保のための技術基準等の在り方
- 各分野内における新たな体制構築へのサポートなど、事業者等に対する支援施策の在り方
- 重要インフラにおける取組みの実効性の確保に必要な制度的枠組みの在り方