平成１４年１１月２８日
情報セキュリティ対策推進会議

「重要インフラのサイバーテロ対策に係る特別行動計画」に基づく取組みの推進について

１．経緯

「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、本年3月、各重要インフラ分野における取組状況等についてのフォローアップを実施するとともに、それらの取組強化に向けた検討課題が提示された（参考資料）ところ、これら課題に関する各分野ごとの検討状況とそれを踏まえた具体的方策等について取りまとめたものである。

２．各分野における検討結果の概要

本年3月の情報セキュリティ対策推進会議開催後、4回のＷＧを実施し、また各分野ごとに、検討課題として挙げられていた

① 重要インフラの情報システムに関する現状把握・検証
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
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

について検討を行った結果は、概要以下のとおりである。

（1）事業者の対象範囲の絞込み

分野によっては、社会的影響度、シェア、事業者数等を勘案しつつ重点的に取組みを行うべき事業者の範囲について当面絞り込むこととし、取組みの確実性、実効性を挙げることとした。

（2）重要インフラにおける情報システムの現状評価

各重要インフラ分野における重要な情報システムに関する現状については、所管省庁等からは以下のとおり報告されており、それぞれ重要システムについて基本的に外部ネットワークとの接続を避けるなど、その安全確保に向けた努力がなされているところではあるが、今後の情報システムの更なる発展・拡充の可能性等も踏まえ、継続的な現状把握・検証の取組み等が重要である。

情報通信分野

○ 基幹的なネットワークインフラを供する電気通信事業者については、電気通信事業法に基づく技術基準を遵守しているほか、「情報通信ネットワーク安全・信頼性基

準」に従ってネットワーク機器の監視機能等を整備している。また、全国的にサービス展開するインターネット接続サービス事業者についても、認証システムやファイアウォールの導入とセキュリティ監査等によるその検証を実施。

○ 放送事業者については、ＮＨＫ及び民放キー局５社の放送システム及び放送中継システムは外部ネットワークとは接続されていない。また社内業務用システムについては、ファイアウォールの設置やウイルス対策等によりセキュリティを確保。

金融分野

○ 民間各金融機関はインターネットバンキングなどのサービス提供にあたって、認証システムやファイアウォールの導入等によりセキュリティを確保。

○ 全銀システム及び東京証券取引所のシステムについては、それぞれ会員金融機関等との間で専用回線、独自のプロトコルを使用して接続されており、外部ネットワークとは直接接続されていない。また東京証券取引所のシステムでは電文の暗号化等を実施。

航空分野

○ 航空運送事業者の運航系システムについては、外部ネットワークとは直接接続されていない。またインターネット予約システムについては、ファイアウォールの設置等によりセキュリティを確保。

鉄道分野

○ 列車運行管理システム及び電力管理システム等の制御系システムは基本的に外部ネットワークとは接続されていないことに加え、鉄道用地内に設置され、他のシステムから独立して列車の衝突･脱線の防止機能を果たす保安装置により列車運行の安全性が確保されている。また事務処理系システムについては、ファイアウォールの設置やセキュリティホール対策の実施等によりセキュリティを確保。

電力分野

○ 各事業者の電力供給のための制御系ネットワークについては、基本的に他のシステムから独立していることに加え、外部ネットワークとは接続されていない。またオフィス業務のための事務系ネットワークは多重のファイアウォールの設置等によりセキュリティを確保。

ガス分野

○ ガス導管網は全国規模でネットワーク化されているものではなく、ガスの製造や供給に係る制御系システムもそれぞれの事業者ごとに他のシステムから独立したものとなっており、自営専用回線の利用等外部ネットワークへの直接接続を回避することによりセキュリティを確保。

地方公共団体関係

○ 各種の情報システムの安定的な稼動･運用が可能となるよう、システム上の措置の確認、検証等を含め、各地方公共団体におけるセキュリティ監査等の対策の実

施を促進するとともに、各団体等間を結ぶ広域ネットワークである総合行政ネットワーク等については、その情報システムに関する技術的な基準等を定め、各団体等に徹底。

(3) 検討課題への具体的方策等

① 重要インフラの情報システムに関する現状把握・検証

事業者等及び所管省庁においては、上記(2)の現状を踏まえつつ、引き続き、外部ネットワークとの接続の有無等情報セキュリティに関するチェックリスト等の策定とその活用、事業者団体加盟各社に対する調査、サイバーテロを原因とする事故・障害発生に関する一定のシナリオの作成とこれを前提とした定性的なリスク分析等の実施などを通じて、重要な情報システムの現状の把握、検証を推進していくこととしている。

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

事業者等及び所管省庁においては、既存の報告・連絡等の枠組みを活用するとともに、業界団体内における協議会等の活用、チェックリスト等の策定とその活用、事業者等に対する調査やヒアリングの継続的な実施等を通じて、情報セキュリティポリシーの策定状況、実施・運用状況の把握、確認等を行うなど、各事業者の取組みの把握を推進していくこととしている。

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

事業者等及び所管省庁においては、従来の検査・監査等における情報セキュリティ対策の観点の導入、緊急時対応計画の策定、第三者等によるセキュリティ監査の実施、事業者間の情報共有化の枠組み構築、官民の合同検討会の開催、研修等の実施による人材の育成・啓発活動などを通じて、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の方策を引き続き推進していくこととしている。

3. 今後の予定等

今回取りまとめられた検討課題①～③に関する具体的方策等について、今後、各分野ごとに所要の体制等を構築しつつその確実な実施を図るとともに、将来的な技術基準の在り方等検討課題④(その他政府における検討事項)についての検討を引き続き進めることとし、適宜、情報セキュリティ専門調査会及び情報セキュリティ対策推進会議を開催し、各省庁からその取組状況・結果等について報告を行うこととする。