資料３

第２次行動計画見直しの方向性について

１．経緯と現状認識

（１）第２次行動計画策定の経緯と現状

重要インフラ行動計画は、重要インフラ防護に責任を有する政府と重要インフラ事業者等が自主的な取組みを進めるにあたっての共通の行動計画であり、重要インフラの情報セキュリティ対策に関する施策の根幹を成すものとして策定されている。

２００５年に策定された第１次行動計画は、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し、政府及び重要インフラ１０分野等からなる関係主体による取組を進めてきた。この結果、２００８年度末までに、「指針」の策定、及びこれに基づく分野毎の安全基準等が策定されるとともにその定期的な見直しサイクルが確立された。また、セプターの整備が完了し、分野間の相互依存性解析及び具体的なシナリオに基づく分野横断的な演習を定期的に実施した。

２００９年に策定された第２次行動計画は、第１次行動計画が初期の目標を計画期間内に達成されたことを踏まえ、第１次行動計画における主な施策を引き続き実施するとともに、刻々と変化する社会環境や技術環境に的確に対応するため、新たに「環境変化への対応」という施策を追加して策定された。第２次行動計画の計画期間中における施策面の主な事柄は、次のとおりである。

①　安全基準等の整備及び浸透

各分野における安全基準等の浸透及び継続的改善について、毎年の調査を通じてその状況を把握するとともに、分野横断的な情報セキュリティ対策をまとめた「指針」の見直しを２回実施した。さらに、対策項目の具体例を記載した「対策編」を策定した。

②　情報共有体制の強化

行動計画により関係主体を定め、検証レベル、実施細目やリエゾンの設定などにより、情報共有体制の大幅な充実が図られた。また、セプターカウンシルが発足、活動を開始し、重要インフラの各セプターによる分野横断的な情報共有や最新の情報収集、意見交換等が行われている。

③　共通脅威分析

重要インフラ分野に共通する各種の脅威について、特に注目する事項を抽出して毎年実施（調査項目例：クラウドコンピューティングの導入、システムの堅牢性）している。

④　分野横断的演習

分野横断的な重要インフラ防護対策の向上を目指し、具体的な IT 障害を想定したシナリオによる演習を毎年実施しており、参加組織数も着実に増加している。

⑤　環境変化への対応

関係機関や重要インフラ事業者との意見交換、最新の IT 環境の調査等のリスクコミュニケーションを充実するとともに、国際的な連携も推進している。

（２）第２次行動計画期間前後における主な環境変化

第２次行動計画が策定された２００９年以前では、PC へのウイルス感染、Winny などの共有ソフトによる情報流出などが社会的な注目を浴びていたが、重要インフラサービスの提供に影響を及ぼすようなサイバー攻撃などに対する認識は、深刻なものではなかった。しかしながら、第２次行動計画期間に入ってから後、政府機関や重要インフラ事業者への DDoS 攻撃、標的型攻撃メール等による情報の流出など

情報システムに対する実際の障害事例も見受けられるようになった。また、制御システムにおいても、Stuxnet によるイランの原子力関連施設への感染・障害が報じられるなど、サイバー攻撃による重要インフラサービスへの影響を意識せざるを得ない状況が出現しつつある。このため、一昨年の東日本大震災発生時に明らかになった課題への対応を含め、ＢＣＰ等の充実、環境変化を踏まえた安全基準の改善等を柱とする行動計画の改定を昨年４月に行った。

また、スマートフォンの急速な普及や東日本大震災被災時の教訓から講じられた対策を元に、クラウド化や BYOD 等の新たな利用形態が進展し、スマートメーター、スマートシティ等の構想により多くの機器が”M2M”、センサーネットワークを介して相互に接続されつつあるなど、情報通信システムやネットワークをとりまく環境は大幅に変化しており、重要インフラサービスに対するリスクの内容や質も変化しているものと考えられる。

さらに、２０１０年に定められた「国民を守る情報セキュリティ戦略」では大規模サイバー攻撃事態における政府の初動対処の整備が求められ、初動対処に係る訓練の実施や平素からの情報共有体制の構築、強化が進められているが、IT 障害はその発生前に何らかの予兆を有することが多いことから、情報セキュリティ対策のために重要インフラ関係者が従来構築してきた情報共有体制を併存して活用することも求められている。

（３）今後の見直しの方向性

重要インフラ行動計画は、２００５年の策定以来、第１次、第２次と重要インフラ分野における情報セキュリティ対策を着実に進展させてきており、

① 安全基準等の整備及び浸透
② 情報共有体制の強化
③ 共通脅威分析
④ 分野横断的演習
⑤ 環境変化への対応

という、第２次行動計画の各施策は有効に機能しているものと考えられる。したがって、次期行動計画において、これらの施策群により構成される基本的な骨格は引き続き維持することが適当である。

その上で、重要インフラ分野における情報セキュリティ対策をさらに発展させるべき詳細項目を検討し、必要な補強を行うことが適当である（具体的な検討課題（例）については別紙に示す）。

別紙

検討課題（例）

（１）重要インフラサービスの定義、対象

「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」として、現在１０分野１５セプターを対象として、各分野を所管する関係省庁とともに取り組みを進めている。

・重要インフラ防護に関する主体の関係機関等への追加
・重要インフラ分野の見直し（施策の推進主体の加除等）

（２）安全基準等の整備及び浸透

現在の対策編では、具体的な対策項目を記載しているが、具体的な対策そのものを例示も含めて詳細に記載するには至っていない。（詳細に過ぎる記載により、分量が不必要に増加することは回避すべきとの考え方あり。）

・対策編自体または別途ガイドラインなどによる具体的内容、例示の記載の是非
・度合いが異なるリスクに対する対策の記載方法

（３）情報共有体制の強化

①　情報連絡・情報提供に関する実施細目

具体的な様式や基準を定めて情報連絡・情報提供を行うことは、一定基準以上の情報を効率的・効果的に共有する手段として非常に有効であることから、実施細目による情報共有は引き続き継続し、その個別の記載については必要に応じて適宜修正することとする。

・これまでの運用を踏まえた点検項目（例）
　別紙１　重要システムの例示
　別紙２　検証レベルと実際の報告との関係
　別紙３　脅威の例
　別紙５　連絡体制

②　セプターカウンシル

改定第２次行動計画において、事業者間で相互に役立つ情報の共有を期待する旨記載を追加したが、カウンシルにおいて具体的な情報共有プロジェクトを推進するに至っている。

・今後、一層の活動の充実のために期待されるカウンシル運営の在り方

（４）共通脅威分析

サイバー攻撃による被害やＩＴ障害が広がりをもっているなかで、情報セキュリティ全体のリスクや情報セキュリティ以外のリスクについても検討する視点を有することが望ましいものと考えられる。

・重要インフラにおける情報セキュリティ対策を考える上で想定されるリスクを意識しつつ、情報セキュリティ全体のリスクや情報セキュリティ以外のリスクをどう考えるのか。また、これらのリスクが重要インフラにどのような影響を与え得るのか。

（５）分野横断的演習

第２次行動計画においては、「リスク（障害）に対する共通理解・認識の醸成」「他分野の対応状況把握による自分野の対応力向上」「官民の情報共有のより効果的な運用方策」を達成するため、重要インフラ所管省庁等が参加する演習として、分野横断的演習のみを記載している。一方で、近年、所管省庁が主催する演習や重要インフラ事業者自らが実施する演習等が実施されている。

・重要インフラにおける情報セキュリティ対策という視点を重視しつつ、横断的演習以外の演習（例：重要インフラ所管省庁等が実施するもの）との連携、協力等をどうすべきか。
・物理的な障害に対応するもの（例：内閣府防災等による訓練、演習）との関係をどの程度意識する必要があるか。

（これら他演習については、連携、協力を検討することが望ましい一方で、事業者の秘密情報等情報共有することが必ずしも適切ではない情報を扱うことも考えられることから、情報共有の程度についても検討することが必要。）

（６）大規模な障害発生時における情報の集約及び共有

現状では、当該事態が発生した場合には、第２次行動計画に定める情報提供・連絡体制にかかわらず、異なる体制で情報の集約・共有を行うこととされている。このように目的的に構築された複数の情報共有体制が存在することから、第２次行動計画の中でも、既存の情報共有体制との間で関係府省庁の協力を得て情報共有の円滑化に向けた検討を行うこととされている。

現実の障害発生時においては、BCP の発動・実施、システムの復旧、障害による影響の最小化等の対策を進める上で、所管庁の情報セキュリティ部門が日常から構築している情報共有体制、事業者間の情報共有体制などを継続させていくことも重要と考えられる。

・（特に大規模な）障害発生時において、既存の情報共有体制との連携及び NISC を中心とする情報共有体制の活用方策の検討。

以上