資料３

重要インフラの情報セキュリティ対策に係る
次期行動計画の検討状況について

平成２５年１０月４日

重要インフラ専門委員会事務局

1. 現状認識

重要インフラに係る行動計画は、重要インフラ防護に責任を有する政府と自主的な取組みを進める重要インフラ事業者等との共通の行動計画であり、内閣官房情報セキュリティセンター（ＮＩＳＣ）設立以前より、「重要インフラのサイバーテロ対策にかかる特別行動計画（２０００年１２月情報セキュリティ対策会議決定）」が策定される等、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。

ＮＩＳＣ設立後の行動計画については、２００５年に情報セキュリティ政策会議により示された、ＩＴ障害から重要インフラを防護し、重要インフラ事業者の事業継続性を確保するために取るべき対策についての基本的方向性を踏まえ、同年に「重要インフラの情報セキュリティ対策に係る行動計画」（第１次行動計画）が策定された。この第１次行動計画により、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みが進められた。

さらに、第１次行動計画において構築された重要インフラの基本的な情報セキュリティ対策や官民の情報共有の枠組みを基礎とし、国として取り組むべき施策を示した「重要インフラの情報セキュリティ対策に係る第２次行動計画」が２００９年に策定された。第２次行動計画では、第１次行動計画における主な施策である「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析[1]」、「分野横断的演習」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いる。

このように、重要インフラ防護は、特別行動計画から見て１３年間、現行の形態となった行動計画でも８年間の実績を有しており、確固たる情報共有体制の構築を始め、５つの施策に基づく対策が着実に進展する等、一定の効果があったと評価される。

今年度、第２次行動計画は最終年度を迎えており、これまでの施策に基づく行動を評価した上で、６月に決定されたサイバーセキュリティ戦略を踏まえ、来年度から実行する次期行動計画を策定する必要があるが、策定に当たっては、評価等により得られた良好事例、要改善事例等の知見を活かしながら、近年の顕在化・巧妙化するサイバー攻撃の趨勢、東日本大震災発災時の対応を踏まえた知見等を踏まえ、来年度から実施する実効的な行動計画を策定する必要がある。

[1] 第１次行動計画では、「相互依存性解析」という施策名である。

2. 策定に当たっての基本理念

2.1. 基本理念

次期行動計画の策定に当たり、「重要インフラ防護」についての基本理念を明確化し、認識を共有することが必要である。

「サイバーセキュリティ戦略」では、「情報の自由な流通の確保」、「深刻化するリスクへの新たな対応」、「リスクベースによる対応の強化」及び「社会的責務を踏まえた行動と共助」を基本的考え方において整理している。

また、第２次行動計画においても、基本的な方向性として「一義的には重要インフラ事業者等が自らの責任において実施」としていることから、こうした考え方を基本理念として踏襲する。

○情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施

- **重要インフラ事業者等**は**事業主体**として、また**社会的責任を負う立場**としてそれぞれに**対策を講**じ、また**継続的な改善**に取り組む
- **政府機関**は、重要インフラ事業者等の情報セキュリティ対策に関する**取組みに対して必要な支援**を行う
- 取組みに当たっては、事業者等の単独のものだけでなく、分野内の他事業者や他分野の事業者等のものとの**連携をも充実**させる
  （個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは、多様な脅威への対応が万全であることを確認することは難しいため）

また、今までの重要インフラ専門委員会においても、「第２次行動計画における施策群の基本的な骨格は維持する」との基本的方針については了解されているものの、次項で述べるような課題も見受けられることから、第２次行動計画における記載の単なる加除修正にとどまらず、個別の施策やその実施体制等を見直し、将来に向けた実効ある行動計画とするために必要な事項を記載する。

2.2. 考慮すべき課題

課題１　関係者（特に重要インフラ事業者等）における理解、浸透度、能力に関してのばらつきが顕在化しつつある一方、「一義的には重要インフラ事業者の責任で対策を行う」ことに関して、その実行や実行に当たっての意識が不十分なところが見受けられる。

（論点）　重要インフラ防護は、体制としてはかなり成熟度が高まっていることを踏まえ、事業者等の自律性を促進しつつ、事業者等間のばらつきをどこまで、どのように是正することを目指すことが適当なのか。

（方向性）

・事業者等にとって実現が困難な理想論を記載するのではなく、現実を見据え、身の丈に合った「実行可能」なものとする。例えば、「安心があたりまえ」「１００%の完璧を期する」といった実現が困難な表現は避けるようにする。

・事業者等におけるセキュリティ対策の鍵を握る経営層が十分にその必要性を把握できるよう、基本的な項目を冒頭に記載する。

・「専門家」ではない可能性のある関係者が含まれることを念頭に、その関係者（及びその担当者が属する重要インフラ事業者等）に何が求められているか、読んで理解できるものとする。

・事業者等が把握すべき階層化された規程類をパッケージ化し、異動の激しい関係者間でも引き継ぎが容易になる構造・内容とする。

・行動計画策定後も、時々刻々と変化する環境に適切に対応し、適切な情報収集・提供を継続的に行うことを可能とするための広報・公聴活動を一層充実させる。

課題２　顕在化する攻撃、大規模化する災害等、年々深刻化している脅威に関して、適切かつ迅速に対応できる体制や方策が十分に講じられていない懸念がある。

（論点）これらの脅威に適切かつ迅速に対応するためにどのような取組みが官民双方に必要になるのか。

（方向性）

・「重要インフラ防護」とは何を何から防護することなのかを明確にする。

・そのうえで、普遍的な対策と、周辺環境の変化に即応できる柔軟な対策に分けて記載する。

・インターネット空間に存在する重要インフラ事業者の活動が、標的にされたり、踏み台とされたりする可能性があることを認識し、こうした弱点について相応の責任が生じ得ることを一層自覚できるように記載を充実させる。

・重要インフラ事業者等におけるリスクマネジメントの重要性と導入の必要性に関して説明し、次期行動計画では具体的な展開を行うことを記載する。

課題３　重大な障害等が発生した際の対処及びその体制（官民間、官官間）が十分整理されていない。

（論点）　サイバー攻撃、災害発生等による重大障害発生時の官民各機関における、共有・連絡すべき情報の整理、各々の対応の明示及び各機関間の連携体制の強化が必要ではないか。

（方向性）

・（「大規模サイバー攻撃」とは何か、明確な定義がない状態ではあるが、）「大規模サイバー攻撃事態」等事業者等にとって特別な警戒を要する事態であると認知するメカニズムを構築する。

・通常状態または通常の障害発生時から大規模障害発生時に至る場合、それまでの対応体制に誰がどう追加されるのかを可能な限り明確化する（なお、事態発生時に全く新しい体制を立ち上げることは現実的でない）

3. 次期行動計画の構成について（案）

3.1. 前回までの施策群についての議論

前回の専門委員会において、第２次行動計画におけるものと同じ施策群を想定したものは、

①安全基準等の整備及び浸透

②情報共有体制の強化

であり、

③共通脅威分析

④分野横断的演習

⑤環境変化への対応

については、施策を構成する内容が変化（増加）することを念頭に更なる検討を行うこととしていた。

③については、それぞれの重要インフラに生じ得る障害等を引き起こすリスクを可能な限り包括的に把握し、その対応策の効果的な活用

④については、所管省庁、事業者等において実施しているものを視野に入れた我が国の演習・訓練の全体像の把握とそれぞれが目指すべき方向性の提示及び防災関係演習・訓練との連携

⑤については、広報・公聴活動、国際連携の推進を引き続き実施することとした上で、その他に必要となる項目

をそれぞれ検討することとしていた。

また、施策群ではないが、「定義と対象範囲」についてもサイバーセキュリティ戦略において求められている取組みとして、現在重要インフラとして位置付けられていないが、そのサービスやシステムにおける機能障害が国民生活及び社会経済活動に多大な影響を及ぼすおそれがある分野における情報システム等の位置付けについて検討し、重要インフラの範囲を見直すこととされていた。

3.2.　次期行動計画において検討が求められる項目

前項までの議論を踏まえ、次期行動計画において実現することが望ましい項目や、その実現に当たり検討が求められるものとして次の点が掲げられる。

施策群等	検討が求められる内容
（定義と対象範囲）	・現在、重要インフラとは位置付けられていないが、現行１０分野と同等にその機能障害が国民生活及び社会経済活動に多大な影響を及ぼす分野におけるシステム、サービスについての位置付けを踏まえた重要インフラの範囲の見直し等 ・システムベンダー、セキュリティベンダー等のサイバー空間関連事業者を関係主体への追加の是非
安全基準等の整備及び浸透	・安全基準等の浸透状況の調査結果を指針・対策編に反映するプロセスの明示 ・指針による成長モデル等の訴求及び対策の実情の調査
情報共有体制の強化	・現共有体制の全体像（第２次行動計画の「別紙４」）における各主体の位置付けの見直し及び各主体間の関係の再整理 ・他分野への波及防止、事例の集積による傾向の分析等に資する情報共有の在り方（脅威の類型等）の見直し ・平時における対応を念頭に置いた対処体制の明確化
分野横断的演習	・重要インフラ所管省庁主催の演習との連携等を通じた関連する演習・訓練の全容の把握及び連携の在り方の整理
環境変化への対応	・（この施策群に含まれる）広報・公聴活動、国際連携の推進を含む施策の在り方 ・情報セキュリティ対策に資する標準・規格の参照の在り方

なお、これらの内容を検討し、行動計画を策定するに当たっては、「2　策定に当たっての基本理念」で述べた基本理念を踏まえたものにする。また、行動計画策定後に周辺状況が大きく変化した場合でも適切に対応できるようにするため、周辺状況を継続的に監視して得られる情報から脅威を特定し、柔軟に対応できる体制を構築する必要がある。

さらに、従来重点が置かれていた未然防止のみならず、障害対応体制の強化に係る記載を充実するとともに、平常時から災害時へのシームレスな対応ができるものとしていく。

3.3.　次期行動計画の骨子案について

これまで述べてきた課題と対応の方向性を踏まえ、次期行動計画の骨子案を以下別添に示す。

別添

次期行動計画の骨子案

1. 重要インフラの定義及び範囲の見直し

現在、１０分野と規定されている重要インフラの範囲の妥当性について検証し、必要があれば、新たに分野の追加、関係主体の追加等を実施。

〇現状と課題

現在、重要インフラとは位置付けられていないが、現行１０分野と同等にその機能障害が国民生活及び社会経済活動に多大な影響を及ぼす分野におけるシステム、サービスについての位置付けを踏まえた重要インフラの範囲の見直し等を図る。具体的には、現在、１０分野と規定されている重要インフラの範囲の妥当性について検証し、必要があれば、新たに分野の追加、関係主体の追加等を実施する。

〇目指す方向性と実現に際し検討すべき課題

当該分野が有する情報システムや制御システムが障害に至った場合の社会・経済に与える影響

- 情報システムの場合　・・・情報サービス提供価値、情報システムが処理するサービスの提供規模
- 制御システムの場合　・・・制御が困難な状態において生じ得るリスクの大きさ
- 共通　・・・既存分野における重要システムに与える影響
  ・・・既存分野との間で認め得る相互依存性
- 既存分野での補強・拡大　・・・既存分野で活動に至っていないものの追加

1.1. 追加候補の絞り込み

候補となる分野・関係主体の中から、実際に参加の打診を行う対象を選定（全体としての選定理由も整理）。

① 分野

② 関係省庁

－分野候補の所管省庁と内閣府防災

－既に実効的に参加している原子力規制庁の正式参加の取扱い

〇現状と課題

東日本大震災等これまでの知見を踏まえ、新たに重要インフラとなり得る分野の候補を数分野に特定している。

一方、当該分野が重要インフラに参加するに当たり、なぜ重要インフラに指定されるのか、参加に見合うメリットがあるのか、といった観点での疑問を払しょくし、自らが活動することの必要性を醸成することが重要な課題である。

〇目指す方向性と実現に際し検討すべき課題

1. 当該分野が有する情報システムや制御システムが障害に至った場合の社会・経済に与える影響

① 情報システム

情報サービス提供価値、情報システムが処理するサービス提供の規模　１分野

② 制御システム

制御が困難な状態において生じ得るリスクの大きさ　２分野

2. 既存の重要インフラ分野における重要システムに与える影響

① 既存重要インフラ分野との間で認め得る相互依存性　１分野

3. 既存の重要インフラ分野での補強・拡大

① 既存重要インフラ分野において、現時点で活動に至っていないものの追加　１分野

1.2. 所管省庁への打診及び規程類の確認

候補となる分野を所管している省庁及び業界団体（セプター候補）に対して、ヒアリング等による感触を打診。参加が見込める状況に至った時点で、ＮＩＳＣの定める施策群にどのように対応しているか、対応する見込みであるかを整理すると同時にセプターの設立について、働きかけを開始。

〇現状と課題

現在合計４分野に対して、説明を行っており、関係省庁で検討中または業界への説明を行っている状況。

〇目指す方向性と実現に際し検討すべき課題

当該分野の参加が見込める状況に至った時点で、業界内の現状を把握し、指導助言を行うとともに、情報共有体制の基となるセプターの設立についても指導助言を行う。

1.3. 新規追加候補分野との関係の整理

各分野の位置付けと共有すべき情報を確認。（既存の分野と同じ扱いで問題ないか否か）

〇現状と課題

２００７年度から情報共有体制が構築され、６年が経過。

現在、１０分野１５セプターに至っている。各セプターは、情報セキュリティ対策の経験時間、業務の性質等から、独自色を有している。また、セプター、事業者の重要インフラ防護に対する取組み姿勢のばらつきが顕在化しつつあることを是正するための方策を考慮する必要がある。こうした中で、新規にセプターが加入した場合、取組みが進んでいる既存セプターの活動に委縮してしまう懸念がある。

〇目指す方向性と実現に際し検討すべき課題

第２次行動計画で明確にされているとおり、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは、多様な脅威への対応が十分であることを確認することは難しいため、分野内の他事業者や他分野の事業者等との連携の充実が重要であることを引き続き継承する。

セプターカウンシルは、相互扶助の精神で新規参入セプターに指導助言を行い、全体の底上げを図ることが必要。

2. 安全基準等の整備及び浸透

2.1. 現行計画の妥当性の検証及び次期行動計画への延長の是非の確認

「指針の継続的改善」、「安全基準等の継続的改善」、「安全基準等の浸透」の既存３施策を次期行動計画でも引き続き実施することの是非を第２次行動計画期間中のまとめとともに確認。

〇現状と課題

サイバー攻撃の高度化等の環境変化、東日本大震災にて生じた複合的障害にて得た教訓等を踏まえ、「指針の継続的改善」については第２次行動計画期間中に２度の改定を行い（第３版（２０１０年度）、第３版改訂版（２０１３年度））、指針の充実・強化を図った。

加えて、「安全基準等の継続的改善」及び「安全基準等の浸透」を通じて、指針と安全基準等の一体的・安定的な見直しサイクル及びセキュリティ対策の推進啓発体制を確立する等、重要インフラ防護に向けて一定の成果を挙げている。

一方、「安全基準等の浸透」を中心としたセキュリティ対策に係る状況確認は、その調査対象の中心が大規模事業者の規定に係る対策状況となっており、中小規模事業者の対策状況、とりわけ具体的な対策状況の把握については困難な状況にある。

加えてサイバー攻撃についてはますます高度化しており、例えば他事業者等を経由した侵入、他事業者等から窃取した可能性がある情報による侵入及びユーザー情報窃取、他事業者等になりすました上でのＤＤｏＳ攻撃等、が見受けられる。

このことから特に中小規模事業者に焦点を当て、具体的な対策状況の把握を通じた具体的な対策向上を軸とした重要インフラ全体での防護能力の底上げを目指す取組みの更なる強化を要する。

〇目指す方向性と実現に際し検討すべき課題

指針と安全基準等の一体的・安定的な見直しサイクル及びセキュリティ対策の推進啓発体制を維持・向上するために、これまでの取組みを強化の上継続する。

加えて、重要インフラ全体での防護能力の強化に向けた「中小規模の事業者等に特に焦点を当てた情報セキュリティ対策の向上策」を新設し、「指針の継続改善」等の既存施策との強化に資することとする。

2.2. 安全基準体系の再整理の検討

平成２６年度に行う指針及び対策編の見直しに関して、関係者がより一層理解しやすいものとするための改定方針を検討。

〇現状と課題

既存の各施策を通じて、安全基準等の策定及び見直しについては一定程度の成果が見られる。

一方、一部事業者等からの安全基準等策定に向けた優先順位付け要望がある等、段階的な安全基準等の策定に向けた支援（指針への記載）を求められている。

〇目指す方向性と実現に際し検討すべき課題

平成２６年度に行う指針及び対策編の見直しにおいては、関係者がより一層理解しやすいものとする。

改定方針については所管省庁及び重要インフラ事業者による実効的な安全基準等の策定・見直しに資することとし、方針に沿った改定内容を検討する。

検討すべき課題については、セキュリティ対策における優先順位付けに係る考え方及び安全基準等策定における成長モデルに係る考え方等の例示に加え、事業者等による優先順位付け及び成長モデルに係る意思決定等のガバナンスの重要性への訴求等とする。

2.3. 下位の計画における質的改善

「安全基準等の浸透状況調査」における実際の対策状況についての確認項目の追加、それらを踏まえた指針・対策編への追加の是非を検討。

〇現状と課題

「安全基準等の浸透度調査」によると、セキュリティ対策に係る状況については一定程度の成熟期に移行しつつあると評価している。

一方で、成熟期における対策状況の確認項目に係る検討、指針・対策編への反映を要する課題抽出機能に係る検討等、重要インフラ全体での防護能力の維持・底上げに向けた見直しを要する。

〇目指す方向性と実現に際し検討すべき課題

「安全基準等の浸透状況調査」を通じて、重要インフラ全体での防護能力の底上げに資する課題抽出、指針・対策編への反映を通じた事業者等へのフィードバック、フィードバック後の対策状況の確認、といったＰＤＣＡ運営、特にＣ（確認）とＡ（是正）に力点を置いた運営にシフトする。

検討すべき課題については、実際の対策状況に係る確認項目の追加、事業者等側の対策プロセス（ＰＤＣＡ）に沿った項目の再整理等に加え、対策退化傾向の検知機能の追加等とする。

2.4. 中小規模の事業者に特に焦点を当てた情報セキュリティ対策の向上策(仮称)

現在実施している「中小規模の事業者に特に焦点を当てた情報セキュリティ対策の向上策（仮称）」は、現行行動計画においては、「補完調査」の一環と位置付けられる。

今後は、実効性の多寡を見極めた上で、在り方を次期行動計画に反映。

〇現状と課題

「安全基準等の浸透」を中心としたセキュリティ対策に係る状況確認は、その調査対象の中心が大規模事業者の規定に係る対策状況となっており、中小規模事業者の対策状況、とりわけ具体的な対策状況の把握については困難な状況にある。

そのため具体的な対策状況の把握に向け、補完調査の一環と位置付けられる往訪による試行調査にて対策状況の把握及びその実効性確認しているところ。

今後、試行調査で得た課題に基づく本施策の企画・実用化を通じて、重要インフラ全体での防護能力の底上げに向けた本施策の安定運用の実現を要する。

〇目指す方向性と実現に際し検討すべき課題

試行調査を通じて得た課題については、指針・対策編への反映等、既存施策を通じて事業者にフィードバックし、事業者による対策を促す体制を目指す。そのために試行及び先行調査の実効性評価及び見直しに基づく本施策の制度設計と実用化を通じた安定運用の実現を要する。

検討すべき課題（現時点の往訪調査にて見えつつある課題）については、経営層のより一層の関与、予防的対策と事後的対策のバランス是正、人材育成やノウハウ蓄積の方策等であり、更に今後の調査にて明らかになった課題を順次追加する。

3. 情報共有体制の強化

3.1. 各主体の位置付けの見直し

各情報セキュリティ関係機関の位置付けの見直し、システムベンダー、セキュリティベンダー、プラットフォームベンダー等新たな関係主体候補の位置付け等、関係機関の範囲の整理を行うことが必要。

これらの各主体との間で共有される情報を整理したうえで、情報セキュリティ関係省庁、事案対処省庁、情報セキュリティ関係機関の位置付けを明確化。

〇現状と課題

障害発生時の連絡体制については、規定する実施細目を２００９年３月に改定し、具体的な実施事項を明示した上で、ＮＩＳＣと所管省庁、情報セキュリティ関係省庁、事案対処省庁、関係機関との間の情報共有を図ってきている。

一方、以下の課題がみられる。

◆ 新たな関係主体候補の位置付け、関係機関の整理

・ＩＴ障害発生時の情報共有の仕組みはあるものの、大規模なものの発生時における明確な情報連携の仕組みまでは整っていない。

・情報共有の仕組みを強化する上で、現状の情報共有体制が定める範囲及び各主体の位置付けでは必要となる情報が明確化されていない。

◆ 共有される情報の整理

・これまでの実績では大規模な事案が発生していないため、所管省庁、情報セキュリティ関係省庁、関係機関とＮＩＳＣとの間の情報連絡・提供で完結していた。

〇目指す方向性と実現に際し検討すべき課題

大規模ＩＴ障害発生時における情報共有を強化する上で、各主体だけでなく、防災も含めた新たな連携を図るための取組みが必要となる。これらの位置付け、役割、情報の整理を行うにあたり、第２次行動計画の別紙４を活用し見直しを行う。

・システムベンダー、セキュリティベンダー、プラットフォームベンダーの追加の是非を検討し、追加する場合の別紙における位置付けを検討。

・大規模災害等を想定した防災関係省庁との連携についての整理。

・ＩＴ障害発生時の情報共有の強化、適切な情報連携を行う上で、重要インフラ分野の追加検討・整理。

3.2. 情報共有機能の強化に向けた共有すべき情報の見直し

所管省庁と事業者との関係を再整理するとともに、ＮＩＳＣへの連絡・提供情報を現在の障害中心の整理に加えて、不正アクセス・攻撃等のリスク関係についても分類可能なよう、「実施細目」の見直し。また、セプターカウシルにおいても、情報共有体制の充実を図るために共有すべき情報や主体間の連携を見直し。

〇現状と課題

共有すべき情報の整理については、政府機関、関係機関、所管省庁、事業者等の各主体に応じて共有すべき情報の抽出と整理をこれまで行ってきた。

障害発生時の連絡体制については実施細目に基づく情報共有の体制が構築され、年々情報共有の件数も増加傾向にある中､第２次行動計画が目指す情報共有が機能してきている。

セプターカウンシルは、重要インフラサービスへの攻撃の未然防止、被害低減、早期復旧を目指し、サイト反応時間の観測プロジェクトの実施や、標的型攻撃に関する情報共有体制の構築を行い、一定以上の成果を上げている。

一方、第２次行動計画では、各主体からの情報連絡をどのように整理し、情報提供を行うかが不明瞭であることから、以下の課題がみられる。

◆ 各主体との関係の再整理

・情報連絡は定常的かつ活発に行われている分野とそうではない分野との差が顕在化しつつある。

・サービスレベル、検証レベルを定義していても、その定義の認識に差異があることや情報連絡に結び付かない場合がある。

◆ 環境変化への対応

・情報共有の目的は、他分野への波及防止及び事例集積による傾向把握等の有益な情報の共有化にある。しかしながら、近年の攻撃手法の巧妙化に伴い、現状の脅威の類型だけでは目的を満たせなくなりつつある。

〇目指す方向性と実現に際し検討すべき課題

障害発生時の連絡体制については、実施細目に基づく情報共有があり機能してはいるが、今後更なる発展、向上を図るための取組みが必要となる。

◆ 各主体との関係の再整理

・各主体との情報のやりとりを整理する上で、実施細目の別紙の見直しを図る必要がある。

・情報連絡件数の開き及び情報連絡体制における認識相違懸念等があることから、認識

の統一を含め、情報の整理・見直しを図る必要がある。

・セプターカウンシルの情報共有体制の充実を図るために、共有すべき情報や主体間の連携の見直しを図る必要がある。

◆ 環境変化への対応

・ＩＴ障害発生時の脅威の分類の見直しを図る必要がある。

3.3. 事案発生時の情報共有体制の整理

現在、大規模サイバー攻撃事態[2]が発生した場合、組織としてのＮＩＳＣの対処態勢が明確ではないことから、平常時の情報連絡・提供体制を維持しつつ、政府全体における対処態勢とどのように連動するのか、事案発生時における対応の推移を含めて検討し、その結果を踏まえ、行動計画に反映。
（なお、本件は、情報共有体制の強化の一環ではなく、別個に整理する可能性あり。）

〇現状と課題

大規模サイバー攻撃事態については、災害やテロ等の緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成１５年１１月２１日閣議決定）に基づき、関係府省庁間で情報を集約及び共有するものとされている。

一方、実際に発生した際の情報共有まで明記されておらず、ＮＩＳＣの対処態勢は明確となっていない。

〇目指す方向性と実現に際し検討すべき課題

平常時の情報連絡・提供体制に加えて、大規模サイバー攻撃事態が発生した際の、ＮＩＳＣの対処体制を政府全体の対処態勢と連携を図るための取組みが必要となる。

[2] 現状明確な定義はない。

4. 障害対応体制の強化[3]

重要インフラ所管省庁が実施するサイバー関係演習・訓練の全体像を把握し、障害対応体制全体の強化を目指す。その中で、分野横断的演習の実施及びセプター訓練を障害対応体制の一環と位置付け、分野横断的演習等の一層の充実を目指すとともに、重要インフラ事業者等に対し演習に関する各種ノウハウを提供できるよう努める。

〇現状と課題

重要インフラ分野の情報システムへの依存度が一段と進み、かつ、情報システムを巡る様々な脅威が一段と顕在化する昨今の状況においては、緊急事態の発生に備えて模擬的な演習を全重要インフラ分野を網羅する官民の各主体が参加の下実施し、相互の情報共有や連絡・連携の仕組みを検証することがますます重要になってきている。ＮＩＳＣの実施する分野横断的演習はそのような演習枠組みを提供する我が国唯一の取組みであり、第１次行動計画期間中の平成１８年度より毎年実施してきている。

一方、各省庁では重要インフラ事業者等を対象に事業者単体でのサイバー関連の対処能力向上を目指した演習・訓練を主催するようになってきている。また、ＮＩＳＣにおいても、セプターの情報共有体制強化の一環で行われている「セプター訓練」が行われてきている。さらに、政府においても、物理的障害発生を想定し政府機関内での初動対処を検証する訓練も実施されている。

このようなＩＴ障害対応を検証する各種演習・訓練について、相互の関係を把握しつつ、分野横断的演習、セプター訓練及び重要インフラ所管省庁の演習・訓練について一層の充実を図ることが必要である。

〇目指す方向性と実現に際し検討すべき課題

分野横断的演習は、民間事業者たる重要インフラ事業者が主体となって実施し、ＮＩＳＣ等関係省庁がサポートするものであり、各分野、複数省庁にまたがる課題を演習に反映しているため、我が国においては、唯一無二のものである。

分野横断的演習のこれまでの実績を踏まえ、引き続き重要インフラ分野の障害対応体制を強化する中核的な取組みとして分野横断的演習を位置付け、他の演習・訓練と互いに連携・補完し相乗効果を発揮できるよう実施していく。その際、重要インフラ防護策の基本理念が事業者等の自立性にあることに配慮する必要がある。

[3]分野横断的演習を中心としたサイバー関連の訓練・演習施策群

4.1. 重要インフラ関係の演習・訓練の全体像の把握及び方向性の提示

重要インフラ所管省庁が実施するサイバー関係演習・訓練の全体像を把握し、分野横断的演習と各省庁の演習との連携を図る。

〇現状と課題

重要インフラ所管省庁で実施している演習は以下のとおり。

省庁	名称	概要	対象者	実施期間・時期	備考
総務省	ＣＹＤＥＲ－実践的防御演習-	官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力の向上を目的として、職員数千人規模の組織内ネットワークを模擬した大規模環境を用いた実践的なサイバー防御演習	官公庁・大企業等のLAN管理者	Ｈ２４補正～	Ｈ２５は全６回実施予定
	電気通信事業分野におけるサイバー攻撃対応演習	サイバー攻撃等によるインターネットの機能不全に対応するために、複数の電気通信事業者等が参加し演習を行うことにより、高度なＩＴスキルを有する人材を育成し、電気通信事業者間の緊急対応体制を強化	電気通信事業者	Ｈ１８～Ｈ２０	国の施策としては終了 テレコムアイザック推進会議にて継続中
経産省	情報セキュリティ対策推進事業	制御システムに対するサイバー攻撃の脅威を認識し、セキュリティインシデント発生の検知手順障害対応手順の妥当性について検証	Ｈ２４年度は、電力、ガス、ビル分野	Ｈ２４～Ｈ２８	
	電力卸取引市場におけるサイバー演習	卸売り電気業界における経済的損失を最小限にとどめるためのインシデントレスポンスに係る対応体制、連絡体制等の確認検証	電力卸売	Ｈ１８	机上演習 終了済
国交省	重要インフラの情報セキュリティ対策に係る机上演習	高度化・煩雑化するＩＴ障害からの防御を目的とした重要インフラ分野におけるセキュリティ対策評価・検証、関係者の熟度及び対応能力の検証	物流分野（航空・鉄道）	Ｈ１９～Ｈ２１	机上演習 終了済

近年、重要インフラ事業者間やセプター・所管省庁・ＮＩＳＣ等との情報共有・連携対処を主に検証する分野横断的演習のほか、重要インフラ所管省庁では独自に個別重要インフラ分野における基幹システムの実機相当を使用する技術面での対処能力の向上を図る演習・訓練を実施するようになっている。

これらの演習・訓練は分野横断的演習と実施目的や期待される効果が異なっているものの、相互に連携・補完し合いながら実施することにより、効率的かつ効果的に重要インフラの防護能力の向上を図っていくことが期待される。

このため、分野横断的演習と各省の演習との連携を図っていくことが求められる。

〇目指す方向性と実現に際し検討すべき課題

分野横断的演習では重要インフラ事業者間やセプター・所管省庁・ＮＩＳＣ等との情報共有・連携対処を主に検証し、各省の演習では主に重要インフラ事業者において基幹システムの実機を可能な限り使用する等技術面での対処能力の向上を図ることを目指す方向性とし、主な対象者、検証目的の明確化及び相互の連携の在り方について検討する。

4.2. セプター訓練の整理

開始後６年を迎え、内容が充実するとともに、演習・訓練と内容が類似してきている「セプター訓練」について、施策としての位置付けを明確化。

情報共有の一環なのか、障害対応体制の強化の一環なのか、セプター訓練により目指すべきものは何か等を整理することにより、どの施策と連動するのか位置付けを明確化。

〇現状と課題

第２次行動計画の下、セプター全体の情報共有体制の維持・向上の機会として、「セプター訓練」を年１回のペースで実施してきた。その中で、訓練内容の細分化が進み、障害対応を念頭においた、より具体的な情報連絡訓練が求められてきている。

〇目指す方向性と実現に際し検討すべき課題

「セプター訓練」は、主にセプター、ＮＩＳＣ、所管省庁による各分野に閉じた「縦の情報共有」体制の維持・向上を目的とするものであり、今後の継続実施においては、その位置付けを障害対応体制の強化策の一つとして今後の検討を進める。

分野横断的演習は、分野間の「横の情報共有」体制に加え一部関係者に限って「縦の情報共有」体制を検証するものである。参加者の網羅性が高いセプター訓練を分野横断的演習の補完施策に位置付け、演習シナリオの一部をセプター訓練に活用する等、状況に応じた分野横断的演習との連携について検討する。

4.3. 分野横断的演習の充実

演習シナリオの検討、演習の実施を通じて、「分野横断的な脅威に対する共通認識の醸成」や、「他分野の対応状況把握による自分野の対応力強化」、「官民の情報共有をより効果的に運用するための方策の取得」等の目標は引き続き掲げるものとし、普及・浸透策の検討及び他施策との関係・連携の在り方を整理。

〇現状と課題

第１次行動計画から引き継がれた３つの目標の下これまで分野横断的演習を実施し、演習参加者からは概ね高い評価を得てきており、その運営手法や成果の蓄積がされてきている。

一方、重要インフラの障害対応体制強化の観点から、分野横断的演習以外の他府省庁主催の演習や重要インフラ基盤強化策との連携を進めつつ、分野横断的演習自身の充実を引き続き図っていくこと課題がみられる。

〇目指す方向性と実現に際し検討すべき課題

分野横断的演習においては、引き続き、①分野横断的な脅威に対する共通認識の醸成、②他分野の対応状況把握による自分野の対応力強化、③官民の情報共有をより効果的に運用するための方策等を獲得することにより、分野横断的重要インフラ防護対策の向上を目指す。

また、障害対応体制の強化に資する分野横断的演習自身の充実として、これまで蓄積した運営ノウハウ・成果の展開、重要インフラ事業者のＩＴシステム維持に密接にかかわる主体の参画、物理的障害への対応までを視野に入れた取組みの検討を進めていく。

4.3.1 演習成果の分野全体への浸透

演習参加を喚起する取組み及び演習成果の周知活動の充実を図るとともに、演習成果の重要インフラ基盤強化策（行動計画における他の施策）への反映プロセスを確立。

〇現状と課題

過去４年間で演習参加者は着実に増加し、演習を有意義と感じる参加者割合も８割を超えるが、毎年の参加組織の約６割がいわゆる常連であり新たな参加組織は必ずしも多くない。同一事業者が繰り返し演習に参加し習熟度を高めることも必要であるが、演習未経験の事業者等に新たに演習に参加頂く、もしくは演習成果を周知することにより、重要インフラ分野全体に演習成果を普及・浸透させることが課題である。

また、毎年度の演習の評価において必ずしも十分な検証ができておらず、翌年度の演習テーマ設定や運営改善、さらには他の重要インフラ防護施策へ展開する取組みが十分ではなく、演習成果を自身の安全基準やＢＣＰ等に結び付け反映するという動きが取りにくい状況がみられている。

〇目指す方向性と実現に際し検討すべき課題

自組織内での演習実施の促進に向けて、演習成果（参加のメリット）をわかりやすく説明する資料（リーフレット等）を作成・公表を通じた重要インフラ分野全体への周知及び経営者層への理解増進の取組み等を検討する。

個別事業者等での演習実施を支援するために、これまでの演習で蓄積した実施・評価・助言手法をとりまとめ共有化できるよう検討を進める。

また、演習成果の次年度活動への反映や他の重要インフラ防護施策への展開を進めるとともに、継続的に重要インフラ事業者が演習成果を自身の情報セキュリティ対策やＢＣＰ等に結び付け反映できるよう、ＮＩＳＣによる演習結果の評価プロセスについて改善を検討する。

4.3.2 ベンダー等の関与

ベンダー等の演習内での位置付けや検証課題を明らかにし、他の演習参加者との情報共有の範囲等について留意した上で、ベンダー等の関与を検討。

〇現状と課題

重要インフラシステムの保守・運用については、ベンダーがかなりの部分に関与しており、障害の未然防止や障害発生時の被害拡大防止、早期復旧に際してベンダーの連携・協力が必要不可欠になっている。

〇目指す方向性と実現に際し検討すべき課題

「3.1. 各主体の位置付けの見直し」の検討結果を踏まえ、ベンダーの演習への関与の在り方を検討する。

4.3.3　ＩＴ障害対応演習と物理的障害対応訓練との連携

大規模自然災害やサイバー攻撃に伴う物理的な被害を考慮したシナリオを策定し、防災・危機管理関係者の参加をも得て、災害及びＩＴ障害の双方に対応するための演習を実施すべきとの考え方もあり得るが、当面まずは関係部局に対して、防災関係の演習・訓練にＩＴシステムの維持・復旧に向けた取組みを反映するよう働きかけることを通じて、情報セキュリティ関係部局と防災関係部局の連携強化を徐々に進めていくことを検討。

〇現状と課題

現実のＩＴ障害対応時には、物理的障害が発生する状況も想定され、その状況次第で、各省や各企業等の情報セキュリティ部門だけでなく防災・危機管理部門との情報共有が生じる可能性は否定できない。一方、分野横断的演習において防災・危機管理部局等との連携体制の検証は行われていない。

〇目指す方向性と実現に際し検討すべき課題

今後、分野横断的演習において、物理的障害への対応も検証課題として取り扱う場合には、シナリオ作成時に必要に応じ内閣府防災や内閣官房の知見の活用、及び各省や各企業等の防災・危機管理関係者の協力の在り方を検討する。

5. リスクマネジメント

5.1. リスクマネジメントの定義の明確化

重要インフラ事業者等において実施されるリスクに対するマネジメントについては、定義、手法が国際的に規格化され、目的、手法が確立されている。こうしたリスクマネジメントの必要性について、背景とともに説明できるようにしておくことが必要である。

例えば、「社会・経済、そしてその一部を構成するシステム等が単純、独立であったものが、近年、複雑化、相互接続されるようになり、リスク因子の質・量ともに増大してきている。これらリスク因子により生じ得るリスクを分析し、今後の施策の実施・見直しに反映する。」等の目的・意義を明確化して、行動計画にも記載することが必要である。

〇現状と課題

これまでの行動計画においては、環境変化に伴う新たな脅威の分析や各分野に共通の脅威の分析、それら情報に基づくリスクに対する共通理解の促進等実施し、政府機関による支援の観点からは一定の成果を上げた。ただし、リスクマネジメントの枠組みから捉え直すと、これまでの施策はリスクマネジメントにおける一部のプロセスの実施をサポートするものであり、リスクマネジメント全体は各重要インフラ事業者等において実施される必要がある。

〇目指す方向性と実現に際し検討すべき課題

情報セキュリティにおいて、リスクを含むマネジメントシステムは ISO/IEC 27000 シリーズにおいて標準化がされており、こういった標準に基づき重要インフラ分野における情報セキュリティのマネジメントの考え方について整理を行う。

その上で、環境変化に伴う新たな脅威の分析や各分野に共通の脅威の分析、それら情報に基づくリスク共通理解の促進等の継続に当たり、これら施策をリスクマネジメントの枠組みのなかで体系的に整理することで、政府機関による支援と重要インフラ事業者等が主体的に取り組むべき内容を明確化する。

5.2.　政府機関におけるリスクマネジメントの支援

重要インフラ事業者等にとって、リスクマネジメントにおけるプロセスのうちリスク分析を実施する際、自分野以外を含む分野間にまたがった脅威等を考慮することは難しい。そこで、「相互依存性の解析（新しい重要インフラを加えて再解析）」、「ＩＴ依存度の分析（新しい分野、ＩＴ浸透が進んだ既存分野）」、「（社会横断的に）浸透する可能性がある新しい技術・システム（例：スマートコミュニティ、Ｍ２Ｍ）についての将来像の予見及び当該技術・システムが重要インフラに与える影響及びリスクの想定」等の内容を政府機関によるリスク分析への支援として実施する。

〇現状と課題

共通脅威の抽出と脅威の分類を行うとともに、それら脅威をもとに詳細な分析を実施した。また、新たな技術・システムの登場といった環境変化に対し、当該技術・システムの利用状況やそれらに伴う新たなリスク等について調査・分析を実施した。

ただし、共通脅威分析の対象となる脅威（課題）の洗い出しを毎年度に実施しなかった点は、第２次行動計画の記載とのかい離があった。これは、１年という短い経過時点では大きな環境変化がなく新たな脅威が見込めないためであり、毎年度実施の義務化は効率的ではないと判断したためである。さらに、脅威を特定する上で、重要インフラ分野における全分野に波及するという共通性に拘ると、例えば制御系・勘定系・情報系のように、一定の分野にとっては重要な脅威であっても取り扱い難いといった課題もみられている。

〇目指す方向性と実現に際し検討すべき課題

重要インフラの情報セキュリティを取り巻く社会、技術環境は刻々と変化しているため、その環境変化に起因するリスク等の調査は、短期、中長期等視点も考慮したうえで、継続実施する。

環境変化の調査の更なる分析の中に、共通脅威分析や相互依存性解析、ＩＴ依存度分析等を位置付け、各調査の内容や実施タイミング等は結果の効果的な活用の観点から見直す必要がある。

5.3. 分析結果の他施策への反映プロセスの確立

安全基準、情報共有体制等への反映プロセスと時期を明確化。

〇現状と課題

環境変化の調査や共通脅威分析、ＩＴ依存度調査等は、安全基準や情報共有体制、分野横断的演習の検討等に反映されてきた。しかし、調査結果に含まれる機微な情報が場合によっては共有できない等の課題がある。また、情報共有、ＩＴシステムに潜在するリスクに対する共通の理解が及ぶ範囲については検討会や委員会等の参加者に限られる点も課題である。

〇目指す方向性と実現に際し検討すべき課題

分析結果については、引き続き安全基準や情報共有体制、分野横断的演習の検討等への反映を図るとともに、これら他の施策の活動を通じて明らかとなった脅威等を当施策へとフィードバックできるプロセスを検討する。

各施策へと反映される情報の粒度（機微情報の秘匿と情報の有用性のトレードオフ問題）を考慮しながら、広い範囲での情報共有、ＩＴシステムに潜在するリスクに対する共通の理解が達成されるよう、情報の共有範囲の確認や共有手段の多様化等を検討行っていく。

6. 防護基盤の強化

6.1. その他防護基盤の強化に属する施策の洗い出し

２～５に係る施策群以外のものを確認。

〇現状と課題

２～５に係る施策群以外のものとして、第２次行動計画では、広報・公聴活動と国際連携がある。

情報セキュリティには国際的な規格・標準が存在するが、第２次行動計画ではそうしたものを十分に活用し、またはフィードバックできる体制となっていない。

その他、第２次行動計画で期待される結果の評価をより実態に即するようにするために、指標では捉えられない側面を補完的に調査する取組みとして、補完調査を実施している。年度ごとに２～４件（平成２５年度は今後実施予定）の事案について調査を実施し、教訓や気付きを得ている。

一方、得られた教訓等を２～５に係る施策群に反映させる位置付けが行動計画上、不明確となっている。

〇目指す方向性と実現に際し検討すべき課題

２～５に係る施策群の共通基盤的位置付けとして、「重要インフラ防護基盤の強化」が必要である。

その中の具体的施策として、引き続き、広報・公聴活動と国際連携を行うとともに、規格・標準として、情報セキュリティに関する規格・標準を踏まえた行動計画の策定や、その重要インフラ分野への展開を推進するとともに、必要に応じて重要インフラ分野に合わせた規程類の整備について検討する。

補完調査については、結果のフィードバック先等、行動計画全体での位置付けを再整理した上で、引き続き実施していくことを検討する。

6.2. 広報・公聴活動

現行第２次行動計画に定める内容に追加すべきものがあるか否か確認。

〇現状と課題

広報活動として、ＮＩＳＣのＷｅｂサイトを用いて、行動計画に基づき実施した重要インフラの情報セキュリティ対策及びその結果を公表するとともに、重要インフラ専門委員会等の会議資料の掲載を行った。

また、内閣官房から関係省庁や重要インフラ事業者等へ配信しているＮＩＳＣ重要インフラニュースレター等において、国内外のセキュリティ情報の発信を行っている。

公聴活動として、セミナーやフォーラム等の場を活用し、行動計画等の情報セキュリティ政策に関する講演を２００９年度から年５回程度行っている。

〇目指す方向性と実現に際し検討すべき課題

Ｗｅｂサイトやニュースレターを通じた広報や、講演等を通じた公聴活動を引き続き積極的に行っていく。

広報においては、そもそも行動計画の内容をより多くの人々に知ってもらうため、例えば経営層に対してはこの部分を重点的に理解してほしいというメッセージ性の伝わる構成とすべく検討を行う。

6.3. 国際連携

現行第２次行動計画に定める内容に追加すべきものがあるか否か、及びＮＩＳＣで別途策定する「国際戦略」における事項の中で次期行動計画に盛り込むものの有無を確認。

〇現状と課題

国際会合への参加や他国機関等との連携を通じて最新動向を把握し、情報共有を行った。年１回開催される、重要インフラ政策に携わる政府機関が相互の連携について検討を行うＭＥＲＩＤＩＡＮ会合に参加し、日本の情報セキュリティ政策等を紹介するとともに、情報セキュリティ政策の国際的な動向に関する情報収集を行った。

また、国際的な監視警戒ネットワーク（ＩＷＷＮ：Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗａｔｃｈ ａｎｄ Ｗａｒｎｉｎｇ Ｎｅｔｗｏｒｋ）を通じて、セキュリティ情報を把握・共有するとともに、隔年で開催される、世界的規模のサイバー演習（Ｃｙｂｅｒ Ｓｔｏｒｍ）に参加し、重要インフラ分野における国際的な連携を深めた。

〇目指す方向性と実現に際し検討すべき課題

世界的な枠組みだけでなく、日米等の二国間や日ＡＳＥＡＮ等の多国間での連携等、引き続き国際連携を積極的に推進していく。

国際連携を通じて得られた事例やベストプラクティス等について、国内の関係主体への情報発信を強化していくことを検討する。

また、サイバー攻撃は容易に国境を越えることや、サイバー攻撃に関するインシデントの国際的な動向把握が重要であることから、ＮＩＳＣにおける国際連携とその展開だけでなく、民間においても、取組みを海外の同業他社に展開したり、海外の動向把握を行ったり等、国際連携を可能な限り進めていくことを検討する。