重要インフラサイバーセキュリティ対策推進会議

重要インフラのサイバーセキュリティに係る施策の基準等
骨子 - 今後の取組方向性 -

１．司令塔機能の強化

サイバー攻撃の巧妙化・高度化や国家を背景とした攻撃キャンペーンの発生等、質・量ともに増大し続けているサイバー脅威に対し、強固な官民連携・国際連携の下、能動的なサイバー防御を可能とするため、令和７年５月、サイバー対処能力強化法及び同整備法[1]が成立した。同整備法においては、能動的サイバー防御等の取組を実現・促進するため、司令塔機能を強化し、政府を挙げた取組を推進するための体制整備を図っている。

重要インフラ[2]等に対するサイバー攻撃キャンペーンに対しては、政府の司令塔としての国家サイバー統括室が、関係府省庁とサイバー安全保障分野の政策の一元的な総合調整等を行い、政府を挙げた取組を推進するとともに、我が国のサイバーセキュリティに係る官民の対応力を結集する。

こうした取組の一環として、政府は、改正されたサイバーセキュリティ基本法（平成26年法律第104号）に基づき[3]、重要インフラ事業者等[4]が分野横断的に実施すべき対策に係る国の施策について検討を進め、令和８年度に新たな基準（以下「重要インフラ統一基準」という。）を作成する[5]。

２．重要インフラ統一基準の作成

現在、重要インフラ事業者等のサイバーセキュリティ確保に係る必要な取組を示した安全基準等としては、各重要インフラ分野に関する法制度の下、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（以下「安全基準等策定指針」という。）や「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「政府統一基準」という。）等を踏まえ、国による基準やガイドライン、あるいは、業界団体等による業

---

[1] 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）及び重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

[2] 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経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもので、重要インフラ分野に属するもの。

[3] サイバーセキュリティ基本法第26条第１項第３号に基づく国の施策の基準。

[4] サイバーセキュリティ基本法第12条第２項第３号に規定する重要社会基盤事業者等。重要インフラ事業者及びその組織する団体並びに地方公共団体。

[5] サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項（令和７年５月29日　サイバーセキュリティ戦略本部決定）p. 4

界標準やガイドライン等が定められている。

他方で、各分野における取組の評価と改善につながるような具体的かつ統一的な基準はなく、サイバーセキュリティ確保の取組やその水準は分野・事業者によってばらつきが見られる。年々巧妙化・高度化の進むサイバー脅威に対応するためには、重要インフラ事業者等において分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）の徹底が求められる。

そのため、重要インフラ事業者等のそうした取組に関する国の行政機関の施策について、具体的かつ統一的な基準を新たに定め、各分野における国や業界団体等による基準・ガイドライン等への反映、重要インフラ事業者等の取組への反映を進めるとともに、それら関係省庁における施策や重要インフラ事業者等における取組の評価及び改善を図ることにより、重要インフラにおけるサイバーセキュリティ強化の実効性を確保する。

重要インフラ統一基準の作成に当たっては、安全基準等策定指針や政府統一基準等の現行制度、各重要インフラ分野における特性や実情、国際標準規格や諸外国の取組、技術・脅威の動向等を考慮する。

また、重要インフラ事業者等におけるサイバーセキュリティ対策の関連制度として、経済安全保障推進法[6]第３章に基づく基幹インフラ制度において基幹インフラ事業者[7]は、サイバーセキュリティ対策を含むリスク管理措置の実施状況について届出が求められている。加えて、基幹インフラ事業者は、新たに成立したサイバー対処能力強化法に基づき資産届出やインシデント報告等が求められることになる。

重要インフラ事業者等を対象としたサイバーセキュリティ基本法に基づく重要インフラ統一基準の作成に当たっては、これら経済安全保障推進法やサイバー対処能力強化法に基づく基幹インフラ事業者を対象とした制度（以下「基幹インフラ関係制度」という。）との整合や全体調和を考慮することによって、重要インフラ事業者等及び基幹インフラ事業者（以下「関係事業者」という。）にとって過度な負担にならないようにしつつ、関係制度間の構造を明確にし、関係事業者においてより効果的な取組がなされるようにする。

官民の情報共有に関しても、同様の観点から関係制度間の構造を明確にする。これまで、重要インフラ事業者等については、「重要インフラのサイバーセキュリティに係る行動計画」[8]（以下「行動計画」という。）に基づき官民の情報共有体制の構築を図ってきた。他方、基幹インフラ事業者については、サイバー対処能力強化法に基づきインシデント報告を行うこととされている。今後、分野横断的な官民の情報共有をさらに強化し、巧妙化・高度化の進むサイバー脅威に対応するため、情報共有の対象や情報連絡の流れ等、情報共有の在り方を整理し、重要インフラ統一基準や関係制度を含め、より効果的な枠組みとする。

---

[6] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）

[7] 経済安全保障推進法第 50 条第１項に規定する特定社会基盤事業者。

[8] 令和７年６月 27 日サイバーセキュリティ戦略本部決定

３．重要インフラ防護範囲の在り方

重要インフラ事業者等は、サイバーセキュリティ基本法等に基づき、重要インフラサービス[9]の安定的かつ適切な提供のため、自主的かつ積極的なサイバーセキュリティの確保等を図ることを目的として、対象分野及び事業者が定められている。

他方、基幹インフラ事業者については、経済安全保障推進法等に基づき、基幹インフラ役務[10]の安定的な提供を確保することを目的として、対象事業及び事業者が指定されている。

そうした中、基幹インフラ事業者等におけるサイバーセキュリティ確保の重要性が増大していることに鑑み、新たにサイバー対処能力強化法が制定され、基幹インフラ事業者は、サイバー攻撃を受けた場合の政府へのインシデント報告等が求められることとなった。

こうした基幹インフラ事業者におけるサイバーセキュリティ確保の重要性の増大を踏まえ、例えば、現在、基幹インフラのうち重要インフラに含まれていない分野・事業者について、それぞれの特性を踏まえつつ、新たに重要インフラ防護の対象として位置付ける等、重要インフラ防護範囲の在り方の見直しを検討する。

当該検討においては、基幹インフラ関係制度における届出やインシデント報告等に当たって前提となるサイバーセキュリティ対策を含め、重要インフラ統一基準に基づく、分野・事業者横断的に講ずべき基本的な対策の徹底を図り、関係事業者においてより効果的な取組がなされるようにする。

４．施策の評価及び改善の方法

重要インフラ統一基準に基づく取組の評価については、年に１回を目途に、まずは内閣官房が重要インフラ所管省庁（以下「所管省庁」という。）を通じて、各分野の重要インフラ事業者等における取組の実施状況に対する専門的調査を行う。所管省庁は、それら調査結果を踏まえ施策の実施状況を取りまとめる。その上で、所管省庁からサイバーセキュリティ戦略本部に取りまとめ結果を報告し、サイバーセキュリティ戦略本部において、基準に基づく取組の評価を行う。

当該調査結果及び評価結果を踏まえ、所管省庁における各分野の施策や、各分野における重要インフラ事業者等の取組を改善することで、重要インフラ分野全体におけるサイバーセキュリティ水準の引上げを図る。

なお、所管省庁が重要インフラ統一基準に基づき施策を実施するに当たり参照するための詳細事項については、別途ガイドライン（以下「対策基準策定ガイドライン」という。）にて定める。対策基準策定ガイドラインは、重要インフラ統一基準から各分野の

---

[9] 重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。

[10] 国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの。

基準・ガイドライン等への反映を通じて、官民の間で共通理解を形成し、サイバーセキュリティ強化に努めることができるような、実効性のあるものとする。

また、現状、分野・事業者によって、サイバーセキュリティ確保の取組やその水準についてばらつきが見られることを踏まえると、対策基準策定ガイドラインにおいて、例えば、「講ずべき対策事項」に加えて「講ずることが望ましい対策事項」を提示する、あるいは、それら対策事項をレベル別に提示する等のオプションが考えられる。こうした仕組みとすることにより、重要インフラ統一基準に基づく所管省庁の施策の実施、取組の評価と改善を進め、各分野におけるサイバーセキュリティ確保の取組水準の着実なレベルアップが図られるようにする。

５．行動計画の見直し等

重要インフラ統一基準は、重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準を示すものであり、直接的にはサイバーセキュリティ戦略本部が所管省庁に対して提示するものである。

他方、行動計画は、重要インフラのサイバーセキュリティに関する政府と重要インフラ事業者等との共通の取組の方向性を示すものであり、サイバーセキュリティ戦略本部から政府関係機関や重要インフラ事業者等のほか、サイバーセキュリティ関係機関、サイバー関連事業者[11]等に対して広く提示するものであるところ、これらの目的や対象は異なる。

重要インフラ統一基準の作成に当たっては、当該基準と行動計画との関係整理や、重要インフラのサイバーセキュリティに関する政府と重要インフラ事業者等の取組の在り方について改めての整理が必要になると考えられることから、行動計画の見直しもあわせて行う。

上記「２．重要インフラ統一基準の作成」、「３．重要インフラ防護範囲の在り方」、「４．施策の評価及び改善の方法」の検討は令和８年度中に行う。また、行動計画についても、重要インフラ統一基準や基幹インフラ関係制度等を踏まえた見直しを令和８年度中に行うほか、重要インフラを取り巻くサイバーセキュリティの環境変化も踏まえて更なる見直し[12]を行う。

---

[11] インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者。

[12] 行動計画「VI. 評価・検証」及び「VII. 本行動計画の見直し」に基づく見直し。