資料６－１

令和元年７月 19 日
内閣サイバーセキュリティセンター

情報共有の改善に関する具体化について

第 18 回重要インフラ専門調査会において、情報共有体制の改善の具体策の１つとして「重要インフラ事業者等との情報共有に関する手引書(骨子案)」(以下､「手引書(骨子案)」という。) について提案したところ。

今回、「「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく情報共有の手引書(試行版)」(以下、「手引書(試行版)」という。) 案及びその今後の活用策・改善策について検討するとともに、NISC による情報提供の在り方及び重要インフラ事業者等における防護の高度化の検討を行う。

1. 手引書について

1.1. 検討経緯

第 18 回重要インフラ専門調査会において、手引書(骨子案)に関する検討を行った。

重要インフラの情報セキュリティ対策に係る第４次行動計画(以下、「行動計画」という。)が求める情報共有、とりわけ情報連絡については、その解説が十分になされているとは言いにくい面がみられる。こうしたことを改善するため、行動計画に基づく情報共有の考え方、具体的な手順、報告様式、共有された情報の背景、期待する活用方策についての解説など、官民双方向の情報共有を効率的に行うために必須な内容を取りまとめ、関係者間で作り上げていき、共有することが有効な手法と考えられるとしたところ。

これを受け、今回、資料６－２に示す手引書(試行版)案について、審議をいただき、手引書(試行版)を策定することとしたい。

手引書(試行版)の策定後、今年度の分野横断的演習の準備段階から周知に活用するなどして、関係者の方々から積極的な意見・希望をいただき、それらを踏まえ、年度末に成案を作成する。

1.2. 手引書の内容について

行動計画を基に、第 18 回重要インフラ専門調査会 資料 12「情報共有体制の改善の具体策について」の別紙１「情報共有の対象範囲(行動計画から抜粋)」及び別紙２「サイバーセキュリティ協議会と重要インフラ行動計画に基づく情報共有体制の関係」をはじめとして、官民双方向の情報共有に必要な具体的手法を文書化するものとする。

1.3. 検討体制

内閣サイバーセキュリティセンター(以下、「NISC」という。)が主体的に策定するものとするが、実践的な手引書とするため、関係者の意見が的確に反映できる体制が適切と考えられるため、別途検討体制を構築していく。

別紙１

情報共有の対象範囲(行動計画から抜粋)

P9　Ⅱ．本行動計画の要点

①「重要インフラ防護」の目的

重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的とする。

P44　別添：情報連絡・情報提供について

1. システムの不具合等に関する情報

重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報(以下「システム(※)の不具合等に関する情報」という。）には、①重要インフラサービス障害の未然防止、②重要インフラサービス障害の拡大防止・迅速な復旧、③重要インフラサービス障害の原因等の分析・検証による再発防止の３つの側面が含まれ、政府機関等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間及び相互依存性のある重要インフラ分野間においてはこうした情報を共有する体制を強化することが必要である。

なお、予兆・ヒヤリハットでは事象が顕在化していないものの、顕在化した際には複数の重要インフラ分野や重要インフラ事業者等の重要インフラサービス障害に至ることも考えられることから、システムの不具合と同様に、情報共有の対象とすることが必要である。

したがって、本行動計画における情報共有の範囲は、図に示すものとする。

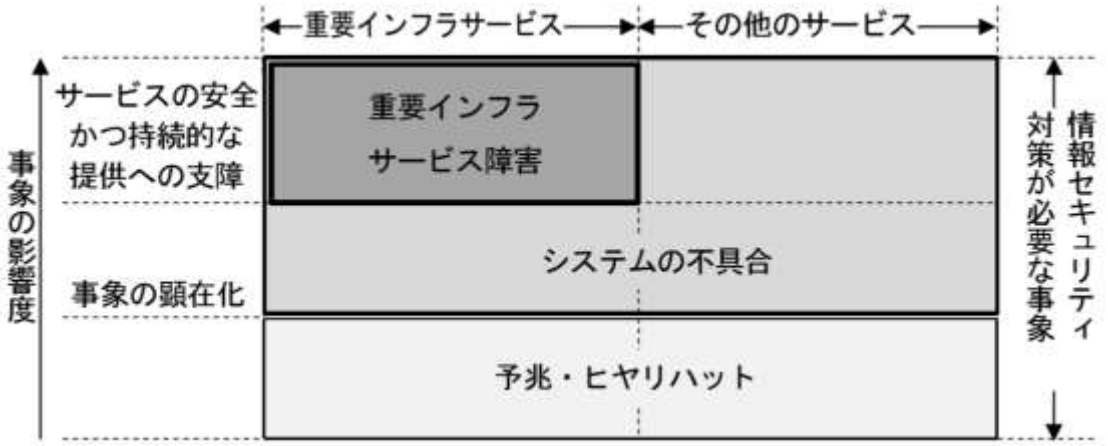
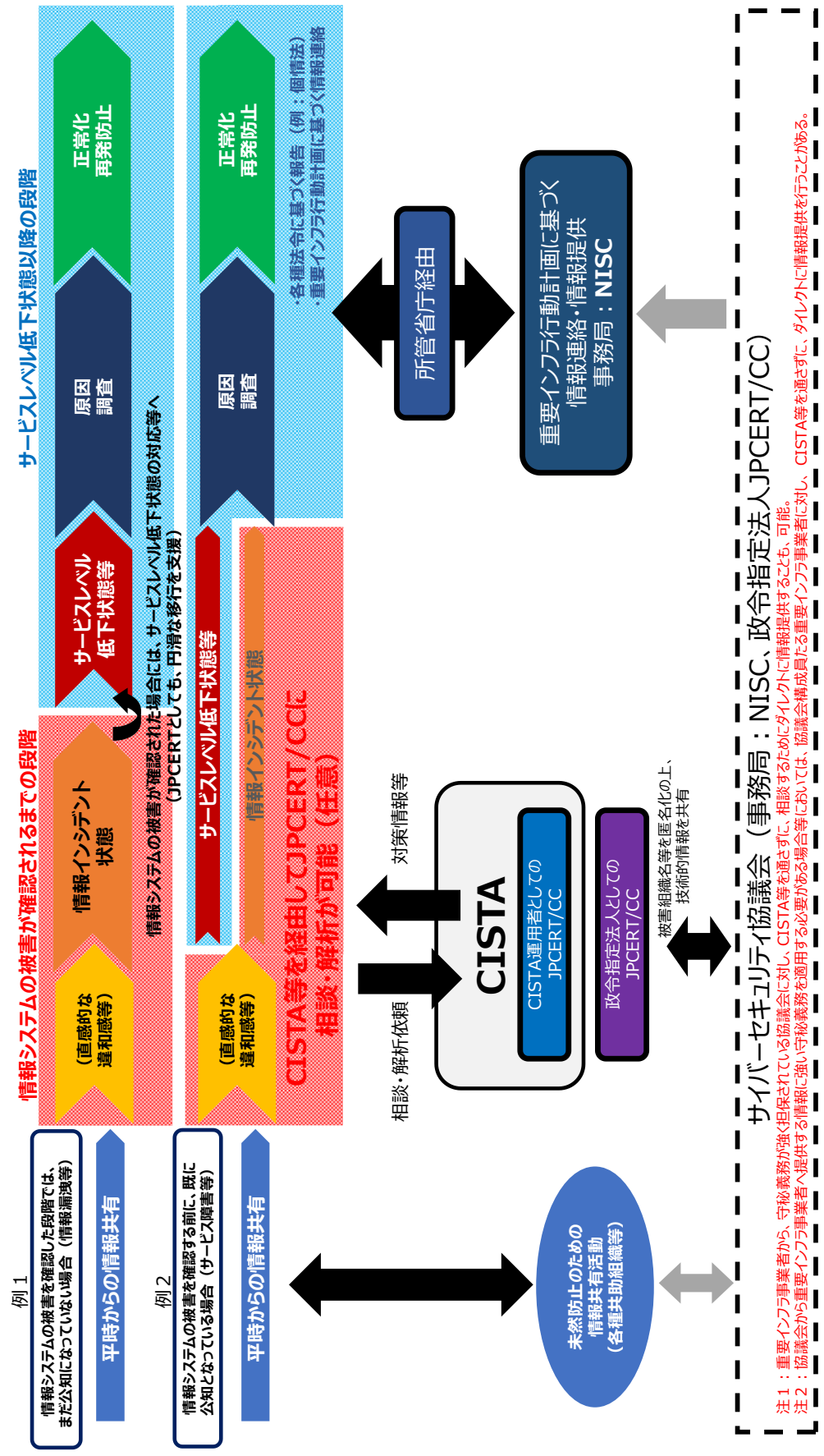


図　情報共有の対象範囲

(※)ここでいうシステムには、いわゆる情報系システムに限らず、各重要インフラ分野のプラントやシステム監視等でも用いられる制御システムや、今後の急速な普及が見込まれるＩｏＴシステム等も含まれることに留意。

別紙２

サイバーセキュリティ協議会と重要インフラ行動計画に基づく情報共有体制の関係



2. NISC による情報提供と重要インフラ事業者等における防護の高度化

これまでの重要インフラ専門調査会での検討において、重要インフラ事業者等からの情報連絡、NISC からの情報提供について、それぞれ課題を明確にし、検討の方向性を示してきたところ。NISC においては、昨年度下半期から、以下の活動を具体化してきた。

- 重要インフラ専門調査会において、事業者等から寄せられた情報連絡から得られた知見のフィードバック、重要インフラを取り巻く国内外の情勢の提供等
- 行動計画における情報提供において、JPCERT/CC からの協力を得つつ、情報分析を踏まえた迅速な情報提供

2.1. 重要インフラ事業者等への情報提供の高度化の試みと課題

NISC からの情報提供は、現行では、パッチマネジメント的なもの、すなわち、機器・システム担当者等への作業指示書的なものとなっている。

他方、年々巧妙化する攻撃者優位な状況となっていることに加え、任務保証に対する目的に対する不確かさの程度としての「リスク」は各事業者等により異なることから、パッチマネジメント的な注意喚起だけでは適切な対応をとれない懸念が生じる状況となっている。

こうしたことを踏まえ、2019 年５月 27 日に情報提供した「外部に公開されたポートに対する攻撃情報に伴う注意喚起」については、公開情報を調査・分析することで得られた最近のサイバー攻撃の状況分析、公知となっている脆弱性、これらの組み合わせにより新たな攻撃の蓋然性が高いと判断したことから、個々の事業者等において、組織全体を俯瞰して検討する目的で発出した。こうした注意喚起は初めての試みであった。

情報提供を行った後、当該注意喚起に示されたサイバーインシデントが発生したことが報告された。結果的に、この判断が適切であったことが示されたことと同時に、当該情報提供が重要インフラ事業者等内で十分に活用されなかったことになる。しかし、情報の受け手側からは、事案を振り返れば理解できるものの、注意喚起を入手した当初は、内容が漠然としており、どう対処してよいのか行動に結び付かなかったとの意見が寄せられた。重要インフラ防護の高度化には、こうした課題について検討することが必要である。

2.2. 重要インフラ防護の高度化について

こうした課題を検討していくため、直截的には、情報提供の在り方、重要インフラ事業者等による活用の在り方の検討が必要と思われる。しかし、その前にもっと広い視野から、どのような方策が適切なのか検討する必要があると考えられる。図に行動計画における「重要インフラ事業者等の対策例」と各施策に関連する「政府機関の施策例」を

示す。

重要インフラ事業者等の防護対策において、年々巧妙化する攻撃者優位な状況を踏まえ、重要インフラ事業者等の「任務保証」の観点から、目的に対する不確かさの程度としての「リスク」をどのようにして、検知して対処するか、いわゆる「リスクマネジメント」を的確に実施できることが求められているところ。これを具体化するものとして、CISO(最高情報セキュリティ管理者)を含めた CSIRT(コンピューターセキュリティにかかるインシデントに対処するための組織)がある。JPCERT/CC 等は、CSIRT を構築・支援するためのガイドを発行しており、こうしたものを活用しながら、それぞれの重要インフラ事業者において最も適切な体制を強化していくことが重要である。

他方、NISC は、行動計画に基づく、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」及び「リスクマネジメント及び対処態勢の整備」の各基本施策を踏まえつつ、どのような情報提供が適切なのか、どのような障害対応体制を重要インフラ事業者に求めるのかを検討していく必要がある。

2.3. 当面の対応

NISC としては、上述の通り情報提供を高度化し、重要インフラ事業者等においては、提供された情報に対して、CISO が組織全体を俯瞰して適切な指示を発することを期待するが、当面の策として、重要インフラ事業者等組織全体で検討する必要がある情報提供を行う場合は、必要に応じて、名宛人を明確にし、それぞれの階層で何を行うべきなのかを明確にすることが適切と考える。

図　行動計画における「重要インフラ事業者等の対策例」と各施策に関連する「政府機関の施策例」