資料 12

平成 31 年４月 18 日
内閣サイバーセキュリティセンター

情報共有体制の改善の具体策について

1. はじめに

第 16 回専門調査会において現状の情報共有体制における課題を整理し、第 17 回専門調査会において改善の方向性について検討したところ。今回は、これまでの審議結果を具現化し、具体的な対策を講じていくための検討を行うものである。

2. これまでの審議のまとめ

重要インフラのサービス障害がクローズアップされる状況となってきている今日、重要インフラのサービス提供の強靭性を高めていくためには、サービス障害が発生した事象から得られる教訓を共有して、運用に生かしていくことが必要である。

このため、「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(平成 29 年 4 月 18 日サイバーセキュリティ戦略本部決定、平成 30 年 7 月 25 日同改定、以下、「行動計画」という。）では、情報共有体制の強化を基本施策に据えているところ。今後、一層の充実強化を行っていくため、現状の情報共有体制における課題を明らかにし、課題に対する対応の方向性について検討してきた。

2.1. 情報共有における課題の整理

第 16 回の専門調査会において、現状の重要インフラ防護における情報共有に関して、サイバー攻撃対応に関心が注がれているが、行動計画で必要とされている人為的ミスや自然災害による重要インフラサービス障害について、情報共有が消極的である傾向があることが指摘された。

重要インフラ防護は、任務保証の観点からサービスの継続的な維持が重要である。このため、サイバー攻撃のみならず、人為的ミスや自然災害による障害情報の活用は、重要インフラサービスの強靭性を高めていくために重要な知見が含まれている。しかし、重要インフラ事業者等からの情報連絡は、サイバー攻撃にフォーカスしている傾向がみられている。なお、自然災害の場合、重要インフラ防護の観点からは復旧優先とし、リアルタイムでの情報連絡よりも、事後の災害を通じて得られた知見の共有が重要である。情報連絡における課題を「表 1 情報連絡における課題」に示す。

他方、NISC から重要インフラ事業者等への情報提供については、リアルタイム性に欠

ける、分野横断的な情報を充実する必要があるなどの課題があげられた。情報提供における課題を「表 2 情報提供における課題」に示す。

表 1 情報連絡における課題

1. 重要インフラ事業者等にとって連絡すべき情報の基準が不明確である。
2. 重要インフラ事業者等にとって情報連絡を行うコストに見合ったベネフィットが得られていない。
3. 重要インフラ事業者にとって、自然災害の場合、重要インフラ防護の観点からは復旧優先とし、リアルタイムでの情報連絡よりも、事後の災害を通じて得られた知見の共有が重要である。
4. 関係省庁にとって報告基準未満の事象であっても、公知となるものについては、報道対応が必要なことから積極的な情報連絡が必要である。
5. 関係者全体にとって情報連絡の活性化には、行動計画に基づく情報共有体制と NISC に関係するその他の情報共有体制との関係を明らかにし、重複箇所の確認や一貫性を出していくことが必要である。

表 2 情報提供における課題

1. 重要インフラ事業者等には、一般的に知られていない段階におけるできるだけ精度の高い情報提供が有益である。
2. 重要インフラ事業者等には、事業者単独では得られない情報、分野をまたいだ情報の提供が有益である。

2.2. 対応の方向性

第 17 回専門調査会において、前項の「表 1 情報連絡における課題」及び「表 2 情報提供における課題」で示された課題について審議を行い、対応の方向性を以下「表 3 対応の方向性について」に示すとおりとした。

表 3 対応の方向性について

1. 重要インフラ事業者等が情報連絡すべき基準の明確化と内容の周知を徹底する必要がある。
2. 公表情報に基づく分野横断的な初期段階の情報などについて、迅速に情報提供していく。
3. 個々の重要インフラ事業者等単独では得られない情報、重要インフラ分野横断的な統計情報等の情報提供を継続的に提供していく。
4. 機微性の高い情報や、事案発生が疑われる段階での情報に関して、事業者が安心して連絡・

相談を行うには、サイバーセキュリティ協議会等の活用を検討していく。

5. 円滑な情報共有を促進するため、行動計画、サイバーセキュリティ対処調整センター、協議会との関係について明確にする。

3. 情報共有体制の改善に向けた具体策について

「2 これまでの審議のまとめ」の課題を踏まえると、重要インフラ防護における情報共有の目的や意義が関係者に十分周知されていないのではないかと推察される。こうしたことから、情報共有の改善に関する具体策を検討する前に、重要インフラ防護における情報共有の目的を明確にし、改善に対する具体策を検討していくこととする。

3.1. 情報共有の目的の明確化

行動計画における重要インフラ防護における情報共有の目的を「表 4 行動計画における情報共有の目的」に示す。

重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、単独で取り組む情報セキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組むことが必要である。また、攻撃者情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じることは、当該攻撃の被害を最小限に留めるだけでなく、新たなサイバー攻撃の抑止にもつながることから、重要インフラ事業者等は共有された情報をリスクマネジメントや事案対処等へ積極的に活用していくなど、情報共有は、重要インフラ事業者等における強靭性の確保のために行うとしている。

したがって、情報共有にコストがかかるといった負担感がみられているのは、情報共有の目的の周知が十分ではないかと推察される。

表 4 行動計画における情報共有の目的

P13 2. 情報共有体制の強化(抄)

重要インフラを取り巻く社会環境・技術環境や情報セキュリティの動向が刻々と変化する中、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、単独で取り組む情報セキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組むことが必要である。また、攻撃者情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じることは、当該攻撃の被害を最小限に留めるだけでなく、新たなサイバー攻撃の抑止にもつながる。

こうした背景を踏まえ、これまでの行動計画でも円滑な情報共有を促進するための取組を進めており、一部の分野では情報共有が活性化するなど一定の成果を得たが、まだ重要インフラ全体として十分な情報共有が行われるまでには至っていない。このため、本行動計画においても引き続き、本件取組の意義・必要性の理解を深め、その活性化を図るための施策を推進することが重要である。

P13 2.1 本行動計画期間における情報共有体制(抄)

我が国ではオリパラ大会をはじめとする国際的なイベントの開催が多数予定されており、重要インフラに対するサイバー攻撃が質・量とも更なる深刻化が想定されるため、関係者間における速やかな情報共有体制の整備が急務となる。第３次行動計画で構築された情報共有体制が関係主体の間で定着していることも踏まえ、これを引き続き継承・発展させ、内閣官房では、以下のとおり情報共有

体制の改善や新たなスキームの検討等に取り組み、重要インフラ事業者等は共有された情報をリスクマネジメントや事案対処等へ積極的に活用していくものとする。

3.2. 行動計画における情報連絡の改善

「3.1 情報共有の目的の明確化」を踏まえ、行動計画に対する関係者の理解を一層促進する方策を検討し、情報共有体制の改善を図ることを検討する。

3.2.1 行動計画に関連する文書の周知

行動計画を的確に関係者が理解し、その考え方に沿った的確な対応がなされることが期待される。このため、サイバーセキュリティ基本法(平成 26 年法律第 104 号、以下、「基本法」という。）を含め、行動計画に基づき重要インフラ防護業務に係る文書体系を明らかにし、業務上必要な時に必要な文書が容易に使用可能な状況とする「関係規程集」を発行し、関係者と共有し、周知活動に活用していく。

3.2.2 情報連絡の具体的な手順の明確化及び周知

行動計画に基づく情報連絡の仕組み、内容、類型等については、行動計画に記載している[1]。分野別の具体的内容については、各分野が策定している「安全基準等」に記載しており、これを基準として情報連絡を行うこととしている。

しかしながら、行動計画が求める情報共有、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基本的考え方、具体的な手順、報告様式、解説など、双方向の情報共有を行うために必須な内容を取りまとめ、関係者間で共有し、作り上げていくことが有効な手法と考えられる。このため、「資料12-2 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）」を叩き台として、次回専門調査会までに同試行版を策定し、これに基づき情報共有の改善に活用していくこととしたい。同試行版策定後、例えば、分野横断的演習に活用するなど、各種周知活動に適用して得られた知見を集約し、年度末には関係者と共に成案を作り上げていくこととし、関係者の周知にも活用することとしたい。

3.2.3 サイバーセキュリティ協議会の活用

行動計画における情報共有対象は、2014 年度から開始した第３次行動計画から引き続き「図 1　情報共有の対象範囲」に示すとおり縦軸に「事象の影響度」、横軸に「重要インフラサービスにかかるシステムか否か」の２次元のマッピングを示し、①重要インフラサービス障害、②システムの不具合、③予兆・ヒヤリハットに区分して運用し、情報連絡を求めてきた。これは、重要インフラサービス障害を未然に防止する観

[1] 行動計画中「別紙３　情報連絡における事象と原因の類型」において、原因の類型として「意図的な原因」、「偶発的な原因」、「環境的な原因」及び「その他の原因」と規定している。

点から、日常業務において、これに至らない事象を幅広く共有することが重要との観点からである。

こうした区分による情報連絡を実施して 5 年近くになるが、情報連絡には、重要インフラサービス障害以外の情報は積極的に寄せられていないことが現状である。この原因としては、日常業務において、システム不具合の前段階の状況が認識されなかったり、状況が認識されたとしても、所管省庁経由で情報連絡することが容易ではないことが推察される。

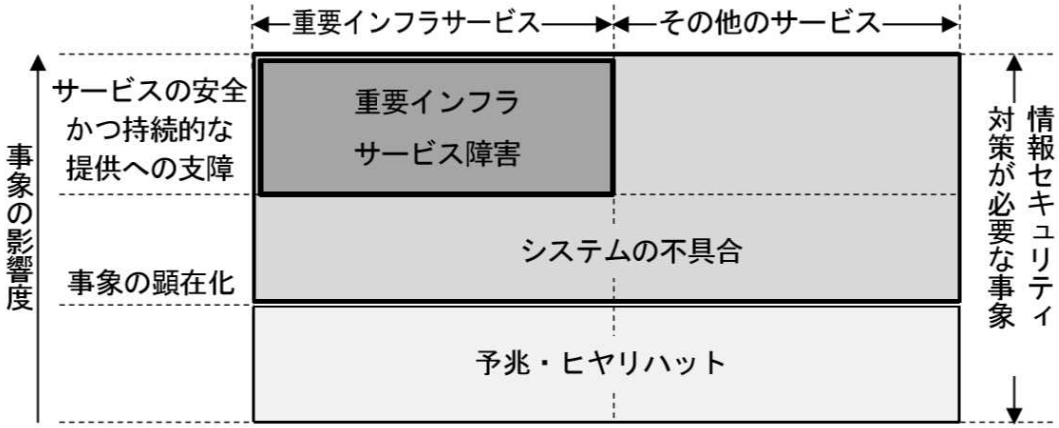

図 1　情報共有の対象範囲

「表 3 対応の方向性について」で「機微性の高い情報や、事案発生が疑われる段階での情報に関して、事業者が安心して連絡・相談を行うには、サイバーセキュリティ協議会等の活用を検討する価値がある。」としたところである。サイバーセキュリティ協議会と行動計画における情報共有体制との関係は別紙２に示すとおりである。

この図において、直感的な違和感や情報インシデント状態が生じた場合、サイバーセキュリティ協議会の相談窓口を活用することにより、守秘義務が担保された状況で、専門家のアドバイスを受け、情報システムの被害が確認された場合には、「図 1　情報共有の対象範囲」に照らして、所管省庁に対しての情報連絡が期待できる。

また、情報インシデント状態が生じ、それが公知となる場合については、より早い段階で所管省庁に対しての情報連絡が期待できる。

こうしたことを踏まえ、情報連絡の改善策のひとつとして、平成 31 年 4 月 1 日に発足した「サイバーセキュリティ協議会」の活用を検討する価値があるのではないか。

3.3. 行動計画における情報提供の改善

2008 年度の「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」開始以降、情報連絡で寄せられる統計情報について、継続的、体系的に収集、保存し、重要インフラ防護に貢献してきたところ。

2018 年度からは、更なる重要インフラ防護の高度化を目指し、国内外の重要インフラを取り巻く状況にかかる開示情報に対する情報収集・分析活動(Open Source Intelligence: OSINT) に取り組んできている。こうした活動により、国内外の重要インフラに関するセキュリティ情報や、事案発生の初期の段階での情報収集によって得られた情報をできるだけ早く重要インフラ事業者等へ情報提供する取り組みを強化してきた。また、重要インフラ事業者等から寄せられた情報連絡を分析し、重要インフラサービス障害事例を一般化し、グッドプラクティスや教訓を四半期ごとに重要インフラ専門調査会において共有してきたところ。今後も引き続き、情報提供の行動化に取り組んでいくとともに、情報連絡及び情報提供が円滑に行われるような施策を行動計画に関係するすべての関係者と対話を通じて高めていく。

4. 具体策案のまとめ

表 5 情報共有の改善に対する具体策案について

＜情報連絡に関する事項＞

- 「関係規定集」の発行
  - 関係規定集を発行し、関係者と共有することにより、行動計画に基づき重要インフラ防護業務に係る文書体系を明らかにし、業務上必要な時に必要な文書が容易に使用可能な状況とする。
- 「重要インフラ行動計画に基づく情報共有の手引き試行版(仮称)」の策定
  - 官民双方向の情報共有を行うために必須な内容を取りまとめ次回専門調査会に試行版を策定し、関係者と共有することにより、周知活動及び日々の情報共有に活用していく。また、試行版の活用によって得られた知見を踏まえ、年度末には成案を策定する。
- サイバーセキュリティ協議会の活用
  - 行動計画が求める情報共有の対象範囲について、より積極的な情報連絡を促進するため、守秘義務が担保され、専門家のアドバイスを受けることが可能なサイバーセキュリティ協議会の活用の検討を行う。

＜情報提供に関する事項＞

- 行動計画における情報提供の改善
  - 国内外の重要インフラに関するセキュリティ情報や、事案発生の初期の段階での情報収集によって得られた情報をできるだけ早く重要インフラ事業者等へ情報提供する。
  - 重要インフラ事業者等から寄せられた情報連絡を分析し、重要インフラサービス障害事例を一般化し、グッドプラクティスや教訓を四半期ごとに重要インフラ専門調査会において共有していく取組みを継続する。

5. その他

2019年4月1日にサイバーセキュリティ協議会及びサイバーセキュリティ対処調整センターが設立されたところである。2020年東京オリンピック・パラリンピック競技大会を踏まえ、重要インフラ防護の高度化が求められており、関連団体との連携・協働が一層重要となってくる。近年、セプターとは別に、重要インフラの類似セクターごとに有志によって運営される ISAC の設立及び積極的な活動が行われるようになってきたことは大いに評価できる。これらの民間における重要インフラ防護活動との連携については、ISACの設立の趣旨を踏まえ、今後検討していくことが必要と考える。

6. 今後のスケジュール

- ○ 第18回(今回)　：情報共有体制の改善の具体策の検討
- ○ 第19回(2019年７月頃)　：情報共有の手引き試行版の策定
- ○ 第20回(2019年10月頃)　：改善された情報共有体制の実施状況確認及び是正
- ○ 第21回(2020年１月頃)　：改善された情報共有体制の実施状況確認及び是正
- ○ 第22回(2020年３月頃)　：情報共有の手引き書の策定

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。

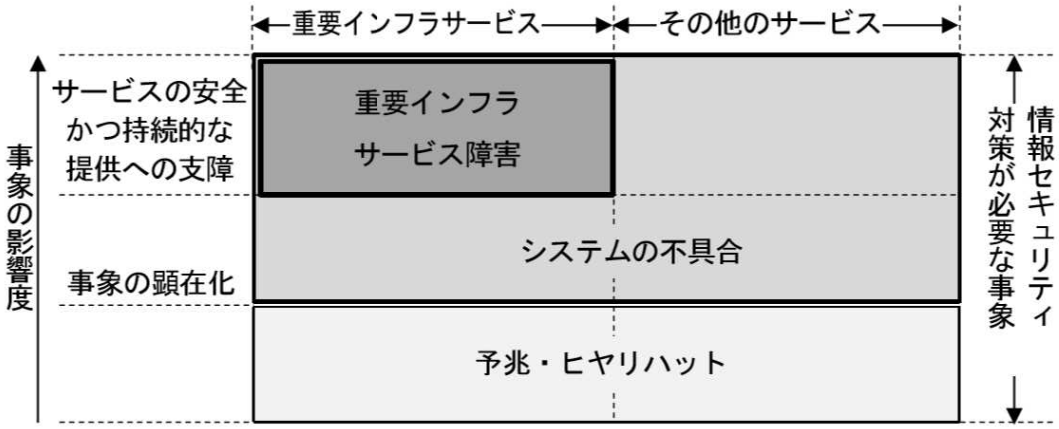

図　情報共有の対象範囲

(※)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。

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