資料６

平成 31 年 1 月 17 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(方向性検討の論点)

１．前回調査会において見出された課題

1.1.情報連絡(重要インフラ事業者⇒NISC)に関する課題

〇情報連絡にかかるコスト
・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ない

〇情報連絡を行う内容
・事業者側から出すべき情報の基準が不明確
・NISC として有益な情報が何であるのかを議論し明確にすべき

〇様々な情報共有体制の関係
・行動計画に基づく情報共有の他に存在する NISC の情報共有体制(協議会やオリパラ CSIRT)との関係を明らかにして、重複箇所の確認や一貫性を出していくべき

1.2.情報提供(NISC⇒重要インフラ事業者)に関する課題

〇情報の性質
・リアルタイムで提供することが重要
・一般的に知られていない段階での情報に価値がある

〇情報の質
・情報連絡を行うコストに見合う情報の質とすべき
・事業者単独では得られない、分野をまたいだ情報が有用である

2. サイバーセキュリティ基本法改正に伴う重要インフラ行動計画に基づく情報共有体制の改善の必要性

サイバーセキュリティ戦略(平成 30 年 7 月)及びサイバーセキュリティ基本法の改正(平成 30 年 12 月)において、NISC として取り組む「従来の枠組を超えた情報共有・連携体制の構築」に示されるように、我が国の新たな情報共有の仕組としてサイバーセキュリティ協議会の全体像を明確にしたところである。

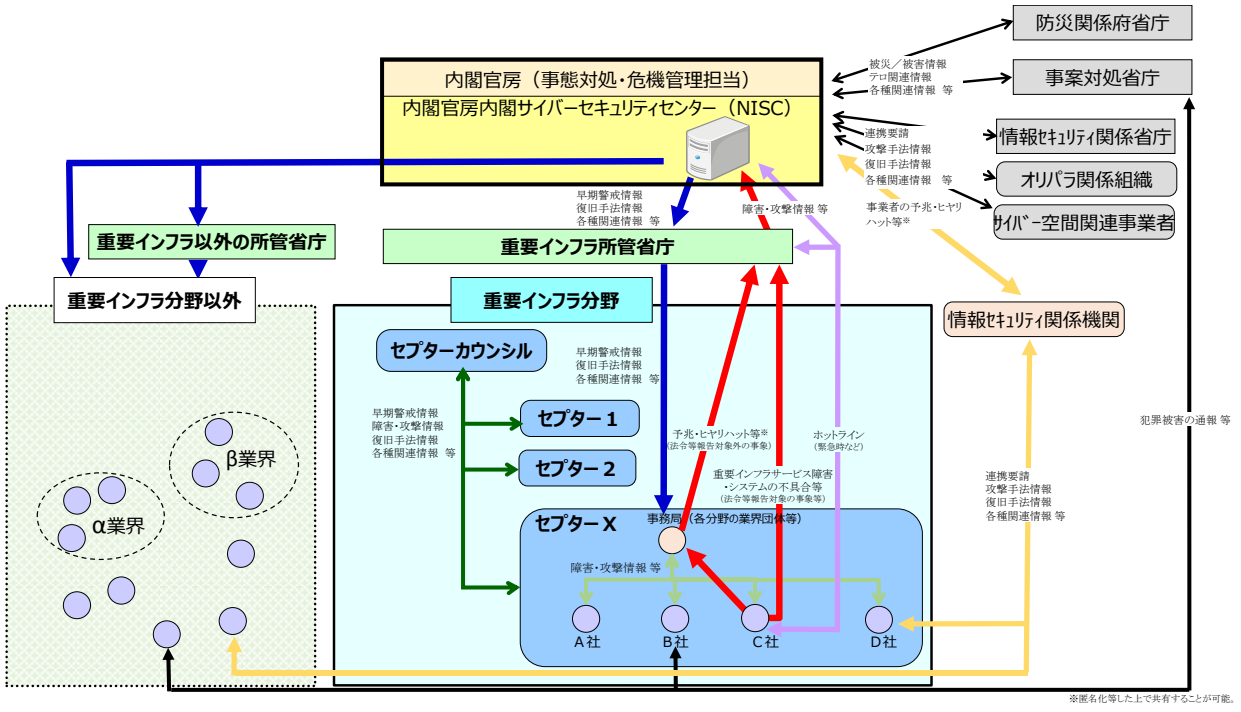
こうした背景を基本として、今後の重要インフラ行動計画の情報共有体制の改善について検討していくこととしてはどうか。

3. 行動計画に基づく情報共有の特徴

重要インフラに関連する情報共有は、行動計画によるもののほか、新たに設置されるサイバーセキュリティ協議会に加え、セプター単位、各 ISAC、C4TAP、J-CSIP、CISTA といった体制が存在している(文末添付図１参照)。こうした情報共有体制と比較して、行動計画に基づく情報共有の特徴は以下の通りである。

● 共有範囲	重要インフラ分野横断的(他にはない特徴)
● 伝達速度	所管省庁を経由するため相応の時間がかかる
● 情報連絡の秘匿性	TLP により設定できるが、所管省庁経由となる
● 情報連絡の根拠	行動計画による(業法で義務付けられたものではない)
● 情報連絡の内容	システムの不具合等に関する情報
● 提供情報の性質	基本的に公開情報に基づくもの
● 継続性	継続的に情報連絡を処理し、統計情報として公表している

行動計画の「別紙４－１　情報共有体制」



4. 改善に向けた検討の方向性

4.1. 情報の特徴に応じた対応の検討

情報の特徴に応じて、情報共有の改善方策を検討してはどうか

- 情報の確度と時間は以下のような関係を適切に使い分ける必要がある

  - 情報の確度は低くても、いち早く共有すべきもの
  - 一定精度が必要なため、共有に相応の時間を有するもの

- いつの時点で、どの程度の粒度の情報の価値が高いか
  同じ情報でも、タイミングによって価値が変わるものと変わらないものがある。
  情報連絡、情報提供においては、次の点に注意して対応する必要があるのではないか。
  - 情報の価値が時間とともに大きく変わるもの
    - ✧ 公表情報に基づく早期警戒情報、ゼロデイ情報など
  - 情報の価値が時間の経過に影響しないもの
    - ✧ 統計情報など

4.2. 重要インフラ行動計画に基づく情報共有の特徴を生かした改善策

行動計画に基づく情報共有体制の長所、短所を踏まえた改善の方向性を検討してはどうか。

■ 長所１　重要インフラ分野横断的にカバーでき、ある程度の速度で伝達することができる

〇 公表情報に基づいた全分野に関係する早期警戒等の注意喚起の充実・強化

- 公表情報に基づいた分野横断的な早期警戒情報、重要アップデート情報、注意喚起情報を適時的確に発信することができる。
- 一層の充実強化には、セキュリティ関係機関、事案対処省庁等との連携強化などが考えられる。

〇 重要インフラサービス障害の初動対応のための情報共有

- SNS の発展により、重要インフラのサービス障害が社会混乱をきたす恐れが強くなってきている。
- 業法による報告対象未満の重要インフラシステムの不具合によるサービス障害であっても、公知のものとなり得るものに関しては、情報の確度は低い段階でも、速報をいただけるとありがたい。

■ 長所２　重要インフラ分野横断的に情報連絡を受け、データを継続して蓄積し、分析している

○ 統計情報の利活用の促進

- 統計を一層充実させることにより、統計データや、グッドプラクティス集の利活用を促進することにより、サイバーセキュリティ対策の強化に資することができる

■ 短所　事業者等が検知した情報で非公表のもの、特定分野に限定されるもの、機微性の高いもの、詳細な内容のものはあまり適さない

○ メンバーシップ制の情報共有体制の活用の検討

- 事業者等が検知した情報で非公表のもの、特定分野間に限定されるもの、機微性が高いもの、詳細な内容のものなどに関する情報共有は、サイバーセキュリティ協議会などのメンバーシップ制を取っている情報共有体制が有利ではないか。
- 事業者における事案発生の疑いの段階での事案の連絡、相談を気兼ねなく安心して行える体制に向いているのではないか。

4.3. **情報連絡(重要インフラ事業者⇒NISC)の改善方策**

○ 情報連絡にかかるコスト低減

- コストの明確化
  - ✧ 原因分析によるコストの明確化
- コスト低減策
  - ✧ 現行の情報共有体制の中でできることはないか(ダイレクトパスの活用等)
  - ✧ インディケータ等、新たな自動情報共有によるコスト低減策の検討

○ 情報連絡すべき内容の周知の再徹底

- 情報の基準が不明確である部分の洗い出しと明確化
  - ✧ 規定されている内容が十分に認識されていない場合がみうけられることから、周知徹底のための方策が必要か。
- 現行の情報共有体制における「安心して情報連絡できる」パスの再認識

○ NISC として有益な情報について

- NISC に期待されることは何か

- その実現のために必要な情報は何か
  - ✧ 例えば、統計処理やグッドプラクティス集によって、サイバーセキュリティの高度化に資することが期待できる。

4.4. 情報提供(NISC⇒重要インフラ事業者)の改善方策

○ リアルタイム性を要求する情報の選定と情報提供要領の具体化

- リアルタイム性を要求する情報の例としては、公表情報に基づく分野横断的な早期警戒情報等が考えられるが、情報の正確性と迅速性はトレードオフになることがある。

- 情報の正確性が高くはないが重要インフラ事業者にとって重要な情報について、どの程度の確度、どの程度の迅速性をもって NISC が情報提供すべきか。

○ 事業者単独では得られない分野横断的情報の具体化

- 例えば、分野横断的な統計情報等に基づく情報提供が考えられるが、この場合、以下を具体化する必要がある。
  - ✧ NISC がこれまで蓄積してきたデータの利活用方策をどう改善していくか。
  - ✧ 統計情報によって得られる分野横断的に発生しうる IT の不具合に対するグッドプラクティス集作成などによるトラブル未然防止対策はどうあるべきか。

5. 行動計画とオリパラ CSIRT との連携について

以下のような運用としてはどうか(文末添付図２参照)。

1. 重要インフラ事業者からの情報提供については、事業者の負担を軽減する観点から、事業者の希望に基づきいずれかに提供すれば他方へも提供したものと見なすことができるようなワンストップ運用とする。
2. 重要インフラ事業者への情報提供については、それぞれの枠組みから展開する（2020 年東京大会までの間は、過渡的に同一の情報が重複して送付される場合がある)。

6. スケジュール

〇第 16 回重要インフラ専門調査会(2018 年 10 月)：済
　現状と問題点、課題の抽出
〇第 17 回重要インフラ専門調査会(2019 年 1 月)：今回
　改善の方向性の検討
〇第 18 回重要インフラ専門調査会(2019 年 3～4 月頃)
　改善された情報共有体制、手順の検討
〇2019 年 4 月　改善された情報共有体制の試行開始

以後、重要インフラ専門調査会ごとに状況を検証し、継続的に改善する。

添付図１

（参考）　既存の情報共有体制の具体例

○現在、NISCをはじめとする政府機関や民間において、以下のような情報共有体制が活動している（代表的なものを紹介）。

- 早期警戒情報の提供システム「CISTA」（JPCERT/CC）
  ※CISTA：Collective Intelligence Station for Trusted Advocates
- 「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」に基づく情報共有体制（NISC）
- サイバー情報共有イニシアティブ「J-CSIP」（IPA）
  ※J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan
- 日本サイバー犯罪対策センター（JC3）による情報共有
- ICT-ISAC、金融ISAC、電力ISAC 等（民間事業者）
  ※ISAC：Information Sharing and Analysis Center

添付図２

オリパラCS対処調整センターとの連携について