資料5

平成 30 年 10 月 29 日
内閣サイバーセキュリティセンター

情報共有体制の現状と課題

1　ねらい

2020 オリパラ東京大会まで 2 年を切った今日、重要インフラのサービス支障がクローズアップされる状況となってきている。こうした状況において、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、サービス支障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、行動計画では、情報共有体制の強化を基本施策に据えており、一層の充実強化が必要である。

2　現状と問題点

行動計画では、機能保証(任務保証)として、自然災害やサイバー攻撃に起因する重要インフラサービス障害の発生の低減と発生時の迅速な対処を求めている。

サイバー攻撃対応に専ら関心が注がれている一方、自損事故による重要インフラのサービス支障も多くみられている。さらに、自然災害に起因する重要インフラシステムの障害も発生している。これらは、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が、報道され公知のものであっても情報共有されないものが散見されている。

なお、事業者からの情報提供は、重要インフラサービス障害(システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。) が対象となっている。

3　解決に向けた方策

現状の情報共有体制について、以下の観点から改善していく方策を検討する。

⑴ **重要インフラサービス障害が発生した際の事業者から NISC への情報連絡の改善方策の検討**

⑵ **NISC から事業者への有用な情報提供の改善方策**

4　検討の進め方

2020 年第 2 四半期にオリパラ東京大会があることを踏まえ、以下のようなスケジュールで検討を行う。

〇第 16 回重要インフラ専門調査会(2018 年 10 月)
　　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 月頃)
　　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 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。

重要インフラの情報セキュリティ対策に係る第４次行動計画における情報共有体制に関する記載

○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

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（抜粋）

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。

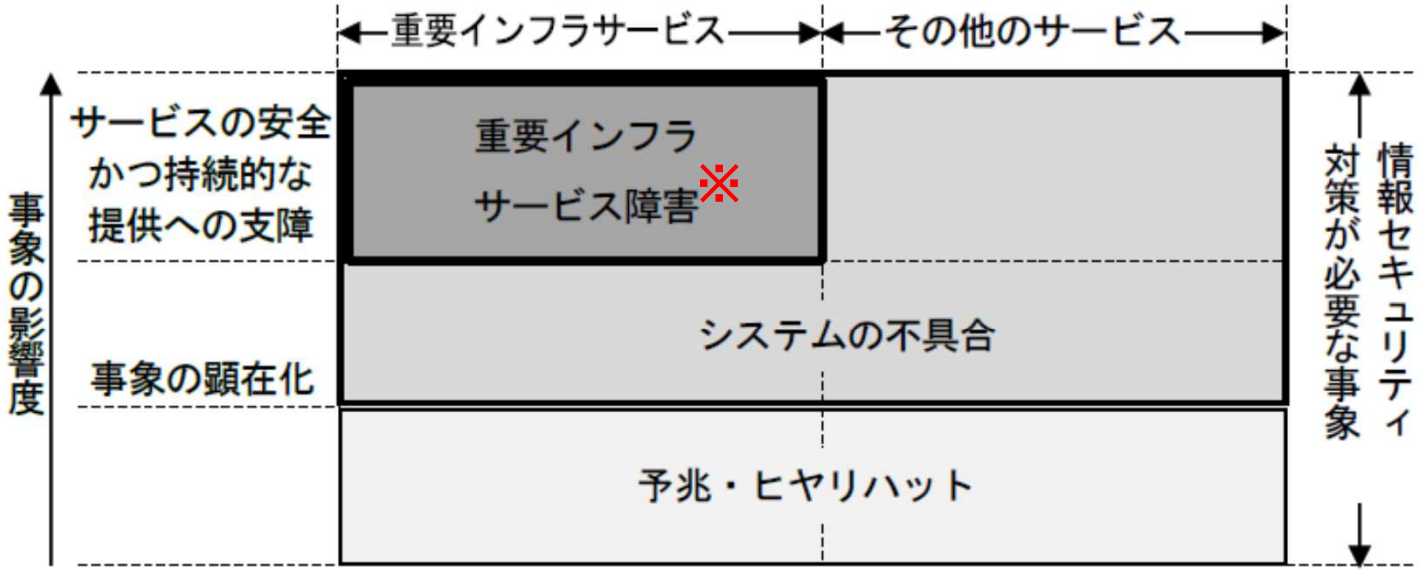


図　情報共有の対象範囲

※重要インフラサービス障害：システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。

○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（続き）

別添：情報連絡・情報提供について
２．重要インフラ事業者等からの情報連絡
２．１　情報連絡を行う場合

システムの不具合等に関する情報のうち、以下のいずれかのケースに該当する場合、重要インフラ事業者等は情報連絡を行うものとする。情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとし、全容が判明する前の断片的又は不確定なものであっても差し支えない。

① 法令等で重要インフラ所管省庁への報告が義務付けられている場合。
② 関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合。
③ そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合。

なお、上記に該当するかどうか不明な場合については、重要インフラ所管省庁又は内閣官房に対して相談することが望ましい。

○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（続き）

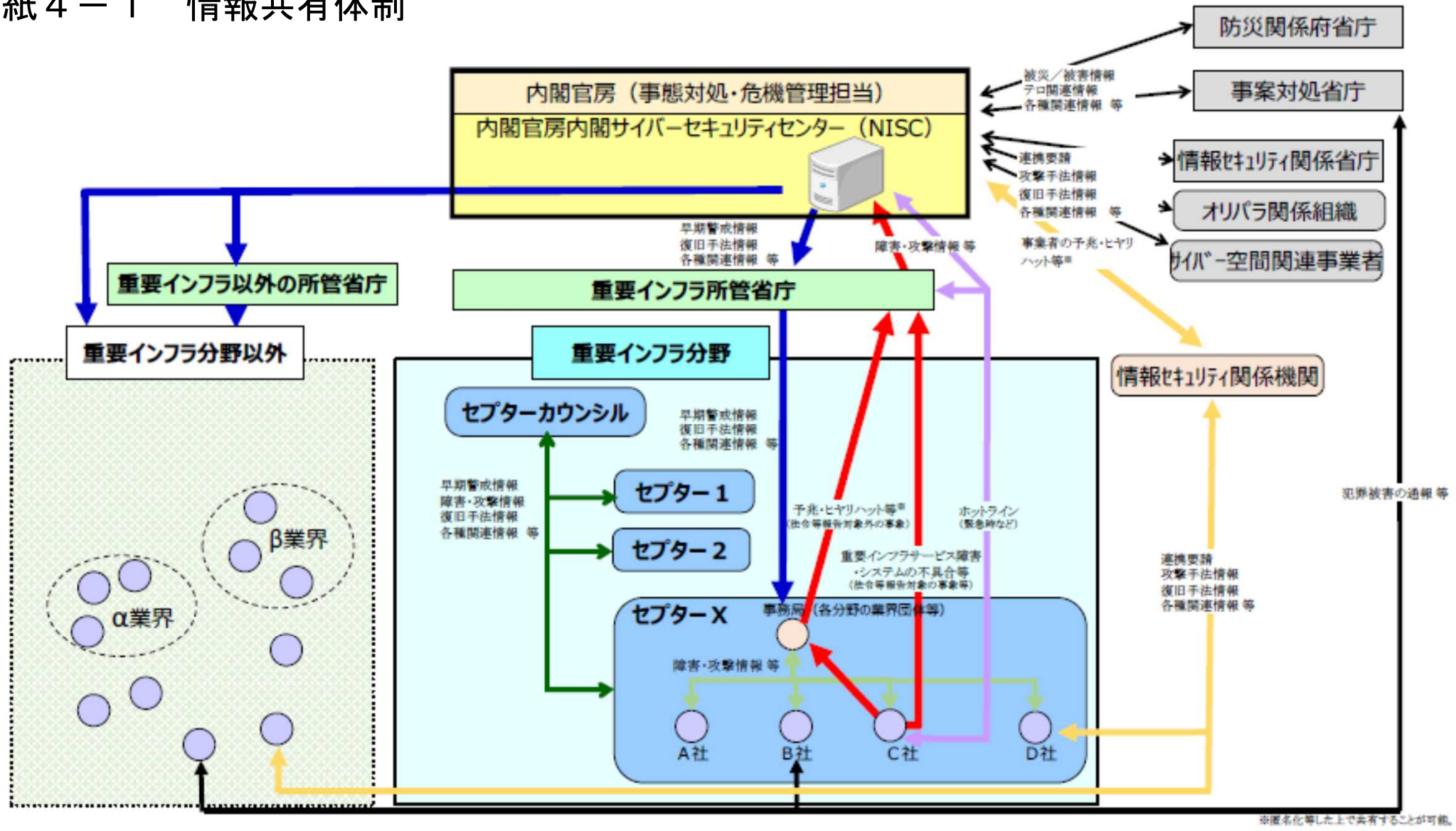
別紙３　情報連絡における事象と原因の類型

事象の類型		事象の例	説明
未発生の事象		予兆・ヒヤリハット	サイバー攻撃の予告等の予兆や、システム脆弱性等の発見、事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信等によるヒヤリハットの発生
発生した事象	機密性を脅かす事象	情報の漏えい	組織の機密情報等の流出等、機密性が脅かされる事象の発生
	完全性を脅かす事象	情報の破壊	Ｗｅｂサイト等の改ざんや組織の機密情報等の破壊等、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やＷｅｂサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記につながる事象	マルウェア等の感染	マルウェア等によるシステム等への感染
		不正コード等の実行	システム脆弱性等をついた不正コード等の実行
		システム等への侵入	外部からのサイバー攻撃等によるシステム等への侵入
		その他	上記以外の事象

原因の類型	原因の例
意図的な原因	不審メール等の受信、ユーザＩＤ等の偽り、DDoS攻撃等の大量アクセス、情報の不正取得、内部不正、適切なシステム等運用の未実施等
偶発的な原因	ユーザの操作ミス、ユーザの管理ミス、不審なファイルの実行、不審なサイトの閲覧、外部委託先の管理ミス、機器等の故障、システムの脆弱性、他分野の障害からの波及等
環境的な原因	災害や疾病等
その他の原因	上記以外の脅威や脆弱性、原因不明等

○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（続き）

別紙４－１　情報共有体制



＜参考＞サイバーセキュリティ戦略

４．目的達成のための施策

４．２．　国民が安全で安心して暮らせる社会の実現

４．２．７　大規模サイバー攻撃事態等への対処態勢の強化

海外では、サイバー攻撃による大規模な停電や金融機関の一部機能停止といった事案が発生し、国民生活に多大な影響を与えている。サイバー空間と実空間の一体化が進展している中、我が国においても、実空間において発生する事案の原因がサイバー攻撃にあることも将来十分にあり得る。また、大規模なサイバー攻撃については、通常、関連性の薄い分野のサービスが同時多発的に被害を受けることも想定されるところであり、係る脅威から国民・社会を守るためには、国が一丸となってサイバー空間の脅威への危機管理にも臨む必要がある。

サイバー空間と実空間の双方の危機管理に臨むために、サイバー空間と実空間の横断的な対処訓練・演習を実施するとともに、当該訓練・演習を通じてサイバー攻撃への対処態勢の強化を図る。加えて、サイバー攻撃に関する分析に係る人材の育成や官民連携の枠組みを通じた情報共有、インターネット観測の高度化を推進し、サイバー空間における情報収集・分析機能及び緊急対処能力の向上を図る。