資料 10－2

「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

令　　和　　２　　年　　３　　月

内閣サイバーセキュリティセンター

更新履歴

日付	内容	文書番号
令和　２年　３月３１日	制定	閣サ第２７５号

目次

Ⅰ．まえがき

１．目的

重要インフラとは、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社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものです。

「重要インフラのサイバーテロ対策に係る特別行動計画」（平成１２年１２月情報セキュリティ対策推進会議決定）において情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）の７分野を重要インフラ分野の対象とし、また、本特別行動計画に基づき平成１３年１０月に官民の連絡・連携体制を構築し、情報共有に取り組んできました。

現在は、「サイバーセキュリティ基本法」（平成２６年法律第１０４号）（以下、「法」という。）第１４条において「重要社会基盤事業者等におけるサイバーセキュリティ確保の推進」として情報の共有を講ずることとしているほか、法第１２条の規定に基づき定めている「サイバーセキュリティ戦略」において重要インフラの防護に関し情報共有体制を拡充していくこととしています。

また、法の基本理念にのっとり策定された「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」（平成２９年４月１８日サイバーセキュリティ戦略本部決定）（以下、「行動計画」という。）において、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油の１４分野を重要インフラ分野と指定しています。本行動計画において情報共有体制について規定しているほか、政府内において、その実施に必要な事項を「重要インフラ所管省庁との情報共有に関する実施細目」（以下、「実施細目」という。）として定め、重要インフラ事業者からの情報連絡や重要インフラ事業者等への情報提供を行っています。

本手引書（試行版）は、重要インフラに係る情報共有の具体的内容、手続き等を明示することにより、重要インフラ事業者等が行動計画に基づく情報共有を円滑に行うための参考にしていただくことを目的にしています。

なお、本手引書（試行版）に記載している内容は一例を示したものであり、ＣＳＩＲＴの構築・改善等、重要インフラ事業者等の自発的な活動を妨げるものではありません。

２．使用上の注意

本手引書（試行版）は、業務をわかりやすく解説することを念頭にし、法令用語等の言い換えを行っている場合もあり、必ずしも正確ではない場合があります。厳密な法令解釈が必要な場合は、法及び行動計画が優先します。

本手引書（試行版）においては行動計画及び細目の記載を引用している部分がありますが、最新の内容に改めている個所もあり、行動計画あるいは細目における記載と一致しない場合があります。

Ⅱ．行動計画に基づく情報共有

１．情報共有について

１．１　情報共有の意義

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す。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つながります。

１．２　情報共有の全体像

行動計画に基づく情報共有は、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。）を重要インフラ事業者等から重要インフラ所管省庁に連絡し、それを重要インフラ所管省庁がＮＩＳＣに連絡する情報連絡と、情報セキュリティ対策に資するための情報をＮＩＳＣから重要インフラ所管省庁に提供し、それを重要インフラ所管省庁が（所管する）重要インフラ事業者等に対して提供する情報提供から成ります。情報共有の流れの概念は図 １ に示すとおりです。本枠組は、サイバーセキュリティ基本法に基づいて構築しているものですが、法令等で義務付けられているものではなく、法第６条に重要社会基盤事業者の責務として規定されている「自主的かつ積極的にサイバーセキュリティの確保に努める」、「サイバーセキュリティに関する施策に協力するよう努める」ということから重要インフラ事業者の協力の下取り組んでいるものです。

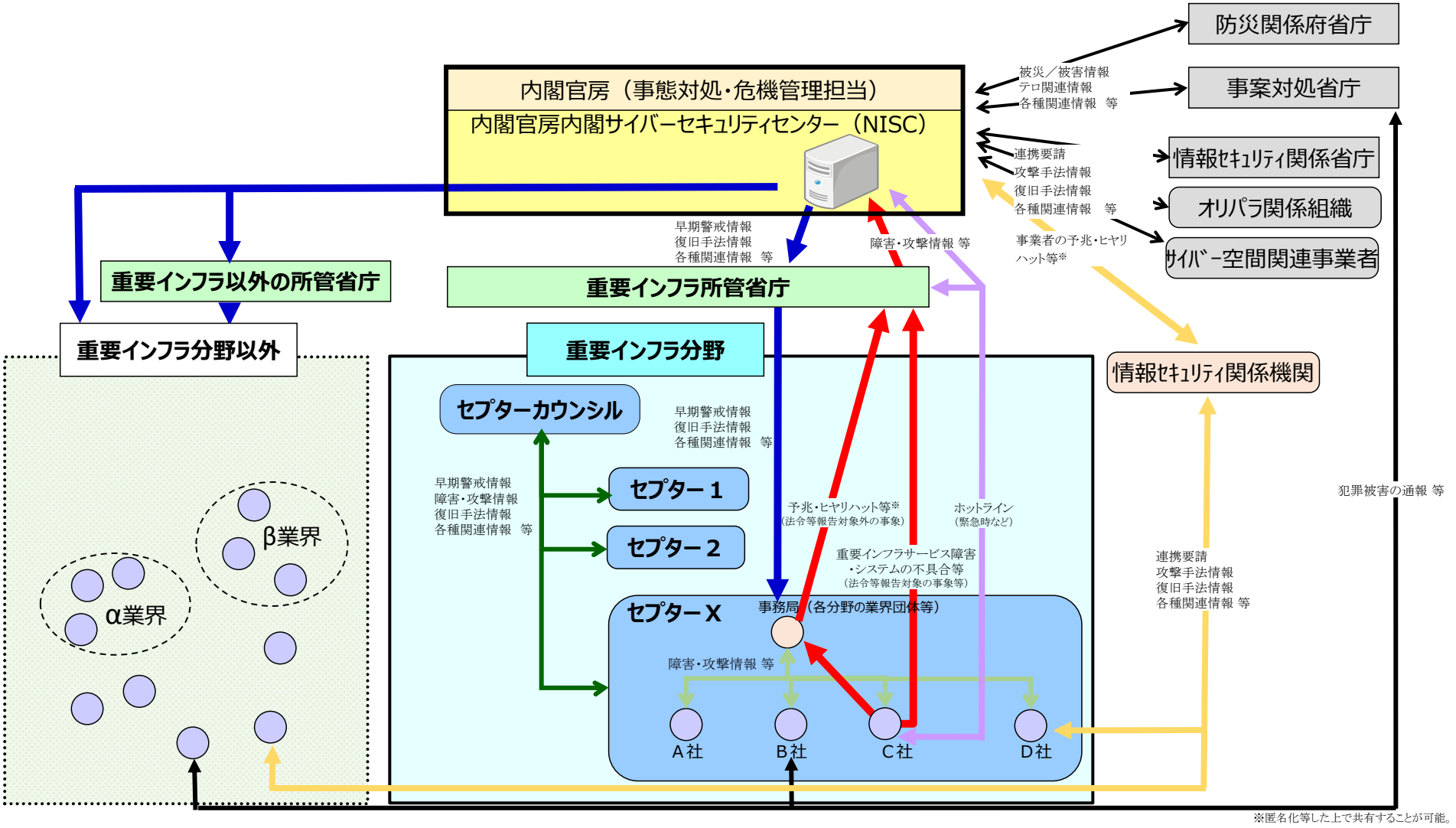

防災関係府省庁
事案対処省庁
情報セキュリティ関係省庁
オリパラ関係組織
サイバー空間関連事業者
内閣官房（事態対処・危機管理担当）
内閣官房内閣サイバーセキュリティセンター（NISC）
被災／被害情報
テロ関連情報
各種関連情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
事業者の予兆・ヒヤリハット等※
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報 等
重要インフラ以外の所管省庁
重要インフラ所管省庁
重要インフラ分野以外
重要インフラ分野
情報セキュリティ関係機関
セプターカウンシル
早期警戒情報
復旧手法情報
各種関連情報　等
早期警戒情報
障害・攻撃情報
復旧手法情報
各種関連情報　等
セプター１
セプター２
予兆・ヒヤリハット等※
（法令等報告対象外の事象）
ホットライン
（緊急時など）
重要インフラサービス障害
・システムの不具合等
（法令等報告対象の事象等）
犯罪被害の通報 等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報 等
β業界
α業界
セプターＸ
事務局（各分野の業界団体等）
障害・攻撃情報 等
A社
B社
C社
D社
※匿名化等した上で共有することが可能。

図 1　情報共有体制

１．３　情報共有の対象

行動計画に基づく情報共有は「システムの不具合等に関する情報」を対象としており、行動計画中以下のとおり規定しています。

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

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て適宜・適切に提供し、また重要インフラ事業者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 2 に示すものとする。

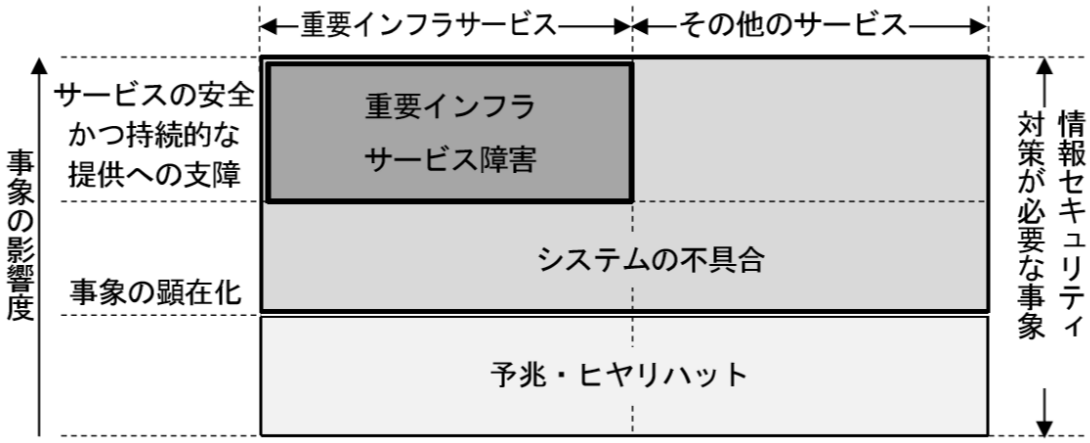


図 2　情報共有の対象範囲

「図 2　情報共有の対象範囲」に示されているとおり、情報共有の対象としているものは事象（結果）であり、その原因については限定をしていません。事象の原因について把握し、分析することが必要かつ重要であることから、情報共有における原因については、その対象はサイバー攻撃のみならず、情報システムに関係するものとしています。①サイバー攻撃等の「意図的な原因」、②操作ミス等の「偶発的な原因」、③災害や疾

病等の「環境的な原因」、④「その他の原因」の４つに分類しています。これは、行動計画に基づき策定されている安全基準等において、重要インフラサービスの安定的供給や事業継続等への影響がないように、顕在化する可能性が高いＩＴ障害を想定した上で、そのＩＴ障害の原因を各重要インフラ分野及び各重要インフラ事業者等の特性等を可能な限り具体的に考慮し規定しているものと同じものです。

①～④の具体的な内容については、各分野が策定している安全基準等において規定している内容を用いることで満たされると考えられます。参考として、その例を表 1 に示します。

表 1　情報連絡における原因の例

原因の類型	原　因	説　明
意図的な原因	不審メール等の受信	標的型攻撃メールやフィッシングメールなどの受信
	ユーザＩＤ等の偽り	パスワードリスト攻撃やＩＤ・パスワードの総当たり攻撃などによるなりすまし
	DDoS 攻撃等の大量アクセス	オープンリゾルバやボットネット等の利用などによる大量アクセス
	情報の不正取得	中間者攻撃やなりすまし等による情報の窃取など
	内部不正	システム運用者等による権限の濫用、盗難や退職者等の権限解除失念等よる不正利用
	適切なシステム等運用の未実施	運用規程等の不遵守、逸脱や適切な規程等の未整備など
偶発的な原因	ユーザの操作ミス	メール誤送信や不適切な権限での情報開示、設定ミスなど
	ユーザの管理ミス	PC や外部記憶媒体(USB メモリ等)等の紛失、盗難など
	不審なファイルの実行	マルウェアに感染した外部記憶装置等の接続やメールの添付ファイル等の閲覧など
	不審なサイトの閲覧	改ざんされたサイトやフィッシングサイト等の悪意あるサイトの閲覧など
	外部委託先の管理ミス	外部委託先による不適切な情報管理やシステム等の運用など
	機器等の故障	ネットワーク機器、ハードウェア機器等の故障（脆弱性以外のソフトウェアの不具合を含む）
	システムの脆弱性	SQL インジェクション等につながる脆弱なコーディング、システムのバグやパッチの未適用などに起因する脆弱性
	他分野の障害からの波及	通信の途絶や停電等の他の重要インフラ分野で発生した障害による影響など
環境的な原因	災害や疾病	地震や台風等による災害やインフルエンザ等の疾病など
その他の原因	その他	上記以外の脅威や脆弱性
	不明	原因を未確認もしくは原因が不明

なお、ここで述べている重要インフラサービスは、重要インフラ事業者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です。各重要インフラ分野における対象となる重要インフラ事業者等と重要システムの例を表 2 に、重要インフラサービスとその障害の例を表 3 に示します。

表 2　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野		対象となる重要インフラ事業者等(注1)	対象となる重要システム例
情報通信		・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融	銀行等 生命保険 損害保険 証券	・銀行、信用金庫、信用組合、労働金庫、農業協同組合等 ・資金清算機関 ・電子債権記録機関 ・生命保険 ・損害保険 ・証券会社 ・金融商品取引所 ・振替機関 ・金融商品取引清算機関　　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・金融機関相互ネットワークシステム ・電子債権記録機関システム ・保険業務システム ・証券取引システム ・取引所システム ・振替システム ・清算システム　　等
航空		・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
空港		・主要な空港・空港ビル事業者	・警戒警備・監視システム ・フライトインフォメーションシステム ・バゲージハンドリングシステム
鉄道		・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力		・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
ガス		・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス		・各府省庁 ・地方公共団体	・各府省庁及び地方公共団体の情報システム （電子政府・電子自治体への対応）
医療		・医療機関 （ただし、小規模なものを除く。）	・診療録等の管理システム等（電子カルテシステム、遠隔画像診断システム等、医用電気機器等）
水道		・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流		・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学		・主要な石油化学事業者	・プラント制御システム
クレジット		・主要なクレジットカード会社　　等	・クレジットカード決済システム
石油		・主要な石油精製・元売事業者	・受発注システム ・生産管理システム ・生産出荷システム　　等

表 3　重要インフラサービスの説明と重要インフラサービス障害の例

重要インフラ分野		重要インフラサービス（手続を含む）（注1）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注2））
		呼称	サービス（手続を含む）の説明（関連する法令）		
情報通信		・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること（電気通信事業法第２条）	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障	・電気通信事業法（業務停止等の報告）第28条 ・電気通信事業法施行規則（報告を要する重大な事故）第58条 【サービス維持レベル】 ・電気通信設備の故障により、役務提供の停止・品質の低下が、３万以上の利用者に対し２時間以上継続する事故が生じないこと
		・放送	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第113条、第122条 ・放送法施行規則（報告を要する重大な事故）第125条 【サービス維持レベル】 ・基幹放送設備の故障により、放送の停止が15分以上継続する事故が生じないこと ・特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が15分以上（中継局の無線設備にあっては、２時間以上）継続する事故が生じないこと
		・ケーブルテレビ	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第137条 ・放送法施行規則（報告を要する重大な事故）第157条 【サービス維持レベル】 ・有線一般放送の業務に用いられる電気通信設備の故障により、放送の停止を受けた利用者の数が３万以上、かつ、停止時間が２時間以上の事故が生じないこと
金融	銀行等	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ（銀行法第10条第１項第１号） ・資金の貸付け又は手形の割引（銀行法第10条第１項第２号） ・為替取引（銀行法第10条第１項第３号）	・預金の払戻しの遅延・停止 ・融資業務の遅延・停止 ・振込等資金移動の遅延・停止	・主要行等向けの総合的な監督指針 ・中小・地域金融機関向けの総合的な監督指針 ・系統金融機関向けの総合的な監督指針
		・資金清算	・資金清算（資金決済に関する法律第２条第10項）	・資金清算の遅延・停止	・清算・振替機関等向けの総合的な監督指針
		・電子記録等	・電子記録（電子記録債権法第56条） ・資金決済に関する情報提供（電子記録債権法第62条及び第63条）	・電子記録、資金決済に関する情報提供の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（12 電子債権記録機関関係）
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付 ・保険金等の支払審査 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針

重要インフラ分野		重要インフラサービス（手続を含む）（注1）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注2））
		呼称	サービス（手続を含む）の説明（関連する法令）		
	損害保険	・保険金等の支払い	・事故受付 ・損害調査等 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針
	証券	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引（金融商品取引法第２条第８項第１号） ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理（金融商品取引法第２条第８項第２号） ・有価証券等清算取次ぎ（金融商品取引法第２条第８項第５号）	・有価証券売買の遅延・停止	・金融商品取引業者等向けの総合的な監督指針
		・金融商品市場の開設	・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務（金融商品取引法第２条第14項及び第16項、第80条並びに第84条）	・有価証券の売買、市場デリバティブ取引等の遅延・停止	・金融商品取引所等に関する内閣府令第112条
		・振替業	・社債等の振替に関する業務（社債、株式等の振替に関する法律第８条）	・社債・株式等の振替等の遅延・停止	・社債、株式等の振替に関する法律（事故の報告）第19条 ・一般振替機関の監督に関する命令（事故）第17条 ・清算・振替機関等向けの総合的な監督指針
		・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
航空		・旅客、貨物の航空輸送サービス ・予約、発券、搭乗・搭載手続 ・運航整備 ・飛行計画作成	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条） ・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・搭乗、航空貨物の搭載 ・航空機の点検・整備 ・飛行計画の作成、航空局への提出	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空分野における情報セキュリティ確保に係る安全ガイドライン
空港		・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）（注1）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注2））
	呼称	サービス（手続を含む）の説明（関連する法令）		
鉄道	・旅客輸送サービス ・発券、入出場手続	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業（鉄道事業法第２条） ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告） 第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第５条 ・鉄道分野における情報セキュリティ確保に係る安全ガイドライン
電力	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条８項） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条14項）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第３条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス	・一般ガス導管事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条第５項）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
	・ガス製造事業	・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であって、その事業の用に供する液化ガス貯蔵設備が経済産業省令で定める要件に該当するもの（ガス事業法第２条第９項）		
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン
物流	・貨物自動車運送事業 ・船舶運航事業 ・港湾運送事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・他人の需要に応じ、港湾においてする船舶への貨物の積込又は船舶からの貨物の取卸の行為等を行う事業（港湾運送事業法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流分野における情報セキュリティ確保に係る安全ガイドライン
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期に渡る製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準

重要インフラ分野	重要インフラサービス（手続を含む）（注1）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注2））
	呼称	サービス（手続を含む）の説明（関連する法令）		
クレジット	・クレジットカード決済	・クレジットカード決済サービス（割賦販売法第２条第３項第１号及び第２号並びに第35条の16第１項第２号及び第２項）	・クレジットカード決済サービスの遅延・停止、カード情報の大規模漏えい	・割賦販売法（後払分野）に基づく監督の基本方針 ・クレジットCEPTOARにおける情報セキュリティガイドライン
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油分野における情報セキュリティ確保に係る安全ガイドライン

注１　ＩＴを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。
注３　表3に記載された内容は令和元年12月現在のものである。法令等の最新の状況については、必要に応じて、所管省庁等へ確認すること。

２．ＮＩＳＣへの情報連絡

２．１　情報連絡の流れ

重要インフラ事業者等において重要インフラサービス障害をはじめとするシステムの不具合等が発生した際において、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重要インフラ所管省庁を通じてＮＩＳＣへ情報連絡を行います。

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。

予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象であるときにも、重要インフラ事業者等から重要インフラ所管省庁に報告を行い、重要インフラ所管省庁がＮＩＳＣへ情報連絡しますが、その他セプター事務局経由で情報連絡元の匿名化等を行った上で重要インフラ所管省庁に報告することも可能です。

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ありません。

重要インフラ所管省庁は、重要インフラ事業者等あるいはセプター事務局からシステムの不具合等に関する報告のあったものについて、情報連絡様式を用いてＮＩＳＣに情報連絡を行います。ＮＩＳＣは、情報連絡を受領した際には識別番号を採番し、提出を行った重要インフラ所管省庁に識別番号を通知します。

情報連絡の流れを図 3 に示します。

ＮＩＳＣへの情報連絡は電子メールを基本としますが、ＦＡＸ及び電話による情報連絡も可能です。

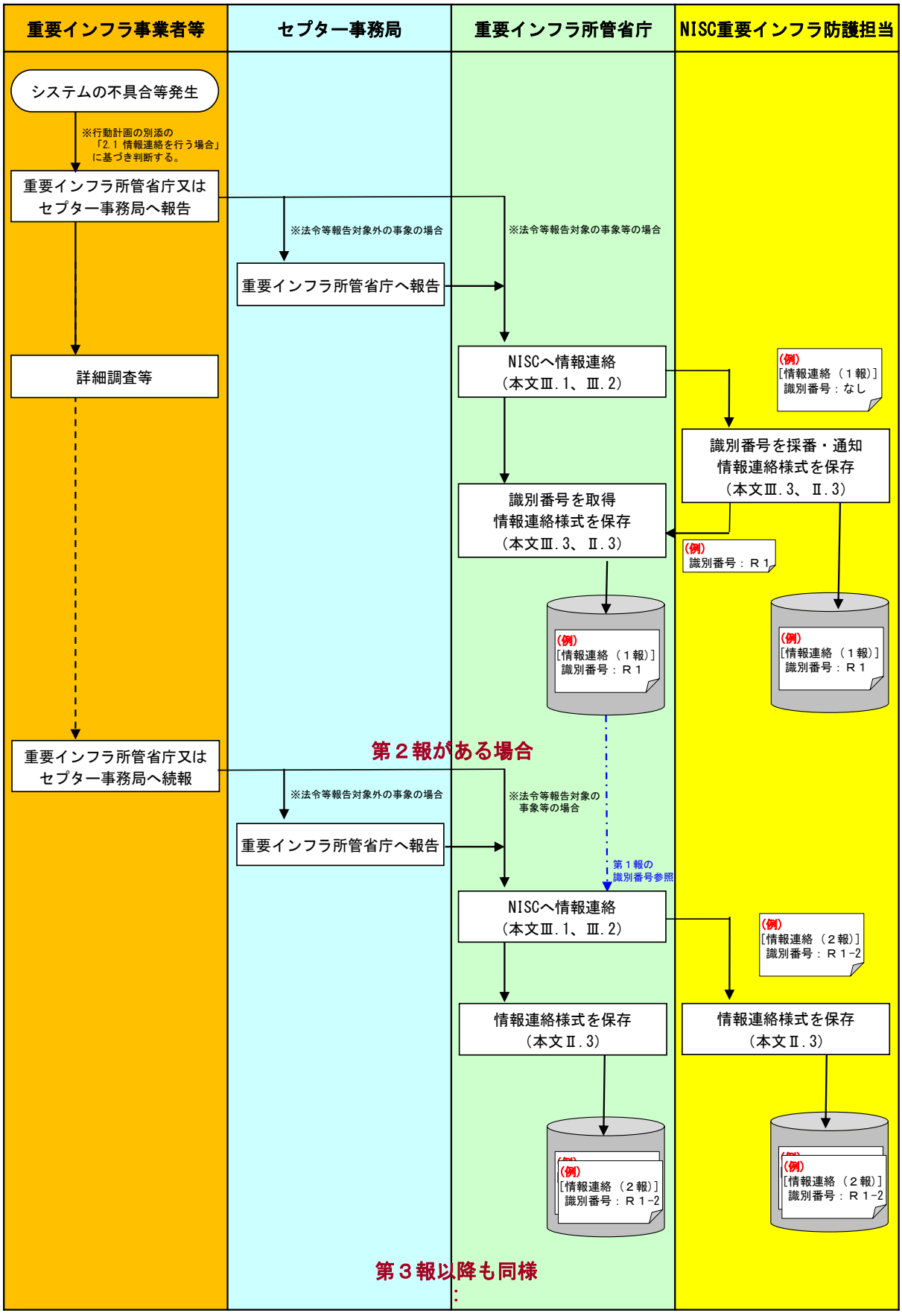

重要インフラ事業者等
セプター事務局
重要インフラ所管省庁
NISC重要インフラ防護担当
システムの不具合等発生
※行動計画の別添の「2.1 情報連絡を行う場合」に基づき判断する。
重要インフラ所管省庁又はセプター事務局へ報告
※法令等報告対象外の事象の場合
※法令等報告対象の事象等の場合
重要インフラ所管省庁へ報告
詳細調査等
NISCへ情報連絡（本文Ⅲ.1、Ⅲ.2）
(例) [情報連絡（１報）] 識別番号：なし
識別番号を採番・通知 情報連絡様式を保存（本文Ⅲ.3、Ⅱ.3）
識別番号を取得 情報連絡様式を保存（本文Ⅲ.3、Ⅱ.3）
(例) 識別番号：Ｒ１
(例) [情報連絡（１報）] 識別番号：Ｒ１
(例) [情報連絡（１報）] 識別番号：Ｒ１
第２報がある場合
重要インフラ所管省庁又はセプター事務局へ続報
※法令等報告対象外の事象の場合
※法令等報告対象の事象等の場合
重要インフラ所管省庁へ報告
第１報の識別番号参照
NISCへ情報連絡（本文Ⅲ.1、Ⅲ.2）
(例) [情報連絡（２報）] 識別番号：Ｒ１-2
情報連絡様式を保存（本文Ⅱ.3）
情報連絡様式を保存（本文Ⅱ.3）
(例) [情報連絡（２報）] 識別番号：Ｒ１-2
(例) [情報連絡（２報）] 識別番号：Ｒ１-2
第３報以降も同様

図 3　情報連絡の流れ

２．２　情報連絡様式

情報連絡様式を図 4、図 5 に示します。

情報連絡様式に記載する事項は次のとおりです。

・報数（当該情報連絡が第何報であるか）
・情報連絡を行う日時
・情報連絡を行う重要インフラ所管省庁担当者の情報
・情報共有範囲
・発生した事象の分類
・発生した事象における原因
・別紙の有無
・分野名
・事象が発生した重要インフラ事業者等の名前
・発生した事象の概要
・重要インフラサービス等への影響に関し、サービス維持レベルの逸脱の有無、他の事業者等への波及の可能性の有無
・当該事象に係る推移等
・今後の予定
・その他、得られた教訓等

重要インフラ所管省庁がこれらの記載を基本的には行います。ただし、予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象の際には、重要インフラ事業者等、あるいはセプター事務局が様式への記載を行った方が正確な内容となりえます。

情報連絡様式への記載例、記載上の注意を図 5 に示します。

なお、迅速な情報連絡を行うことを優先する観点から、得られた情報の範囲で情報連絡資料を作成するものとし、情報の追加や更新の都度、続報を発信するものとします。特に、セプター事務局からの報告については、事業者名をはじめとして匿名化された情報が含まれている場合もあるため、記載可能な範囲で記載することとします。

様式1

☐警報 ☐注意喚起 ☐参考情報

（重要インフラ所管省庁→内閣官房）

情報連絡様式

（第　報*）

（*が付与された項目は必須事項）

識別番号*　（※第1報の識別番号は空欄）

情報連絡日時*　年　月　日　時　分

情報連絡元*	省庁名：		担当者名：	
	部局名：			
	電話番号：		FAX番号：	
	電子メールアドレス：			
情報共有範囲*	☐Red = 宛先限り （NISC重要インフラ防護担当(※1)限り） ☐Amber=特定分野・関係者限り （NISC重要インフラ防護担当(※1)並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り） ☐Green=重要インフラ関係主体限り （NISC、重要インフラ所管省庁、事案対処省庁、情報セキュリティ関係省庁、防災関係府省庁、情報セキュリティ関係機関、オリパラ関係組織、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り） ☐White=公開情報			
	特記事項： 企業名・該当サービス等、企業が特定される事項を除いて他分野への情報提供可。			

※1：情報の集約・分析のため、必要に応じ、あらかじめ連携を要請した情報セキュリティ関係機関との間で情報共有を行う。

①発生した事象の分類

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	☐
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など）	☐
	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など）	☐
	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）	☐
	上記につながる事象(※3)	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	☐

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の分類

原因の類型	原因	チェック（複数選択可）
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	☐
	適切なシステム運用等の未実施	☐
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	☐
環境的な原因	災害や疾病等	☐
その他の原因	その他	☐
	不明	☐

◆情報連絡の内容(※4)　（別紙有無*：☐有　☐無）

項　目	情報の内容
③分野名*(※5)	リストから選択
④事象が発生した重要インフラ事業者等名	
⑤概　要	判明日時：　年　月　日　時　分 （発生日時：　年　月　日　時　分 ） 事象が発生したシステム・委託先業者等： 発生事象の概要： システムの稼働状況：☐影響なし ☐停止中 ☐一部稼働中 ☐復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：☐有 ☐無 他の事業者等への波及の可能性：☐有 ☐無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 （補足情報） 対外的な対応状況 報道発表、報道等への掲載：☐済 ☐予定有 ☐無（済・予定有では日時・件名を記入） NISC以外に連絡を行った先：
⑧今後の予定	☐事象継続中 （続報あり） ☐事後調査実施中 （続報あり） ☐今後の対応策を継続検討 （続報なし） ☐対応完了 （続報なし）
⑨その他・得られた教訓等	

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「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」に定める「分野名」を指す。
※6：「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」に定める「サービス維持レベル」を指す。

図 4　情報連絡様式

参考

□警報 □注意喚起 ■参考情報

（重要インフラ所管省庁→内閣官房）

記載例　：青字
記載上の注意：赤字

情報連絡様式

（第　1　報*）

（*が付与された項目は必須事項）

西暦で記載

24時間表記で記載

識別番号*

情報連絡日時* 2020 年 4 月 1 日 13 時 15 分　（※第1報の識別番号は空欄）

いつ時点での内容かの日付・時間を記載。（記載するとセルの色は白に変化）

情報連絡元*	省庁名：	XX省	担当者名：	連絡　太郎
	部局名：	YY課		
	電話番号：	03-XXXX-YYYY	FAX番号：	03-XXXX-YYYY
	電子メールアドレス：	renraku.taro@xx.go.jp		

情報共有範囲*

□ Red = 宛先限り
（NISC重要インフラ防護担当(※1)限り）

□ Amber=特定分野・関係者限り
（NISC重要インフラ防護担当(※1)並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り）

■ Green=重要インフラ関係主体限り
（NISC、重要インフラ所管省庁、事案対処省庁、情報セキュリティ関係省庁、防災関係府省庁、情報セキュリティ関係機関、オリパラ関係組織、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り）

□ White=公開情報

選択したＴＬＰ（情報共有範囲）に関する補足情報を記載。

特記事項：
企業名・該当サービス等、企業が特定される事項を除いて他分野への情報提供可。

※1：情報の集約・分析のため、必要に応じ、あらかじめ連携を要請した情報セキュリティ関係機関との間で情報共有を行う。

①発生した事象の分類

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	□
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など）	□
	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など）	■
	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）	□
	上記につながる事象(※3)	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	□

最初に明らかとなった事象を、別紙２の説明を参考に１つだけ■を選択する。

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の分類

原因の類型	原因	チェック（複数選択可）
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	□
	適切なシステム運用等の未実施	□
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	□
環境的な原因	災害や疾病等	□
その他の原因	その他	□
	不明	■

発生原因について■を選択する。複数選択可。

◆情報連絡の内容(※4)　（別紙有無*：☐有　■無）

項　目	リストから選択　情報の内容
③分野名*(※5)	○○分野
④事象が発生した重要インフラ事業者等名	○○株式会社　（西暦で記載）（24時間表記で記載）
⑤概　要	判明日時：　2020 年 XX 月 XX 日 XX 時 XX 分 （発生日時：　2020 年 XX 月 YY 日 YY 時 YY 分（サーバログ等より推測）） 事象が発生したシステム・委託先業者等： 会社情報管理サービス（https://example.com/top.php） ・会員がアクセスし、個人情報の変更やサービス申込等を実施。 発生事象の概要： ・○○株式会社の会員情報管理サービスのWEBサイトが改竄された。 ・閲覧したユーザにウイルス感染の恐れがあり、現在、当該サイトを一時閉鎖しサービス停止中。 ・多数の個人情報流出が確認されており、被害の詳細を調査中。 システムの稼働状況：　☐影響なし　■停止中　☐一部稼働中　☐復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：　☐有　■無 他の事業者等への波及の可能性：　☐有　■無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 XX/XX 00:00 / 外部より○○株式会社のHPがおかしいと匿名メールを受信。 XX/XX 01:00 / サーバ運用ベンダへ連絡。サーバログ等の調査をし、HPが改ざんされていることを確認。 XX/XX 03:00 / アクセスした利用者にウィルス感染のおそれがあるためサーバを停止。 （必要に応じて行を追加して経緯を記載。） （補足情報） ・XX月XX日現在、○○件の個人情報流出を確認。 （名前、住所、電話番号、メールアドレスが漏えい。） ・コンテンツ管理システムYYYYのv99.99の脆弱性を突かれたものと想定される。 （報道発表等がある場合は、別紙として添付する、あるいは掲載ページのアドレス等を記載。）
	対外的な対応状況 報道発表、報道等への掲載：　■済　☐予定有　☐無　（済・予定有では日時・件名を記入） XX/XX 09:00頃　○○株式会社のトップページにニュースリリースを掲載。 （https://example.com/newsXXXX） NISC以外に連絡を行った先： XX/XX 10:00頃　○○県警へ通報
⑧今後の予定	■事象継続中　（続報あり） ☐事後調査実施中　（続報あり） ☐今後の対応策を継続検討　（続報なし） ☐対応完了　（続報なし）
⑨その他・得られた教訓等	・現時点での得られた教訓は、経営層への情報のエスカレーション体制を普段から確認し、迅速な判断ができるようにすること。

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「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」に定める「分野名」を指す。
※6：「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」に定める「サービス維持レベル」を指す。

図 5　情報連絡様式記載例

２．３　情報連絡様式中の具体的記載について

本項では、情報連絡様式中、補足説明が必要と考えられるものについて解説します。

(1) 重要度

情報連絡様式において、対策を実施する主体※がとるべき対応に応じて重要度をあらかじめ警報、注意喚起、参考情報の３段階に定義しています。重要度は表 4 の説明を参考に適切なものを選択します。

※対策を実施する主体：情報連絡を受領し、その内容に対して対策を行う者

表 4　情報連絡の重要度及びその説明

重要度	説明
警報	対策を実施する主体において、直ちに対応について検討することが推奨される情報
注意喚起	対策を実施する主体において、対応について検討することが推奨される情報
参考情報	対策を実施する主体に対する情報セキュリティ対策への参考情報

(2) 情報共有範囲（Traffic Light Protocol：ＴＬＰ）

情報連絡に記載する情報には、企業情報や、情報の拡散により脅威が増大するおそれのある機微情報等が含まれることから、情報発信者※は、適切なＴＬＰを設定する必要があります。

※重要インフラ事業者等が重要インフラ所管省庁に報告する際にあっては、重要インフラ事業者等。セプター事務局が重要インフラ所管省庁に報告する際にあっては、セプター事務局。重要インフラ所管省庁がＮＩＳＣに情報連絡する際にあっては、重要インフラ所管省庁。

ＴＬＰによる情報の共有範囲は、

・Red＝宛先限り、即ちＮＩＳＣ重要インフラ防護担当限り

・Amber＝特定分野・関係者限り、即ちＮＩＳＣ重要インフラ防護担当並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り

・Green＝重要インフラ関係主体限り、即ちＮＩＳＣ、重要インフラ所管省庁、事案対処省庁、情報セキュリティ関係省庁、防災関係府省庁、情報セキュリティ関係機関、オリパラ関係組織、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属するもの限り

・White＝公開情報

であり、その定義は表 5 に示すとおりです。

情報連絡様式中に予めＴＬＰの欄を設定していることから適切なものを選択します。ただし、例えば、Red を選択した場合であっても、事象が発生した重要インフラ事業者等がウェブサイトでその内容を発表しており、その内容については共有可能であるなど、ＴＬＰによらない共有範囲がある場合には、その内容を特記事項に記載することになります。

表 5　情報共有範囲

区　分		情報共有可能な範囲(※1)	定義
	Red 宛先限り	・　ＮＩＳＣ（重要インフラ防護担当）※2 ・　重要インフラ所管省庁（情報提供先又は情報提供元の所管省庁）	情報発信者と、情報受信者の２者間に限定する。
	Amber 特定分野・関係者限り	・　ＮＩＳＣ（重要インフラ防護担当）※2 ・　重要インフラ所管省庁（直接関係する分野） ・　セプター（直接関係する分野） ・　セプターを構成する重要インフラ事業者等（直接関係する分野）	左記の情報共有範囲に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）で、かつ業務の遂行にあたって、その情報を知る必要がある者に限る。
	Green 重要インフラ関係主体限り	・　ＮＩＳＣ ・　重要インフラ所管省庁 ・　事案対処省庁 ・　情報セキュリティ関係省庁 ・　防災関係府省庁 ・　情報セキュリティ関係機関 ・　オリパラ関係組織 ・　サイバー空間関連事業者 ・　セプター ・　セプターを構成する重要インフラ事業者等	左記の情報共有範囲に属する者（その組織の職員並びにコンサルタント、その組織内で働いている外部の業務受託者及びセプターを構成する重要インフラ事業者等から委託を受けて情報システムの開発、運用等を行う者であって、秘密保持契約を締結している者）に限る。
	White 公開情報	・　限定なし	要機密情報としての扱いは要さない。著作権を適性に扱う限りにおいて、分配、出版、インターネット上での公開及び放送に供することも可能とする。

※１：情報発信者が、上記の情報共有範囲に含まれない対象の追加を求める場合は、当該対象を共有範囲に含めることができるものとする。

※２：情報の集約・分析のため、必要に応じ、あらかじめ連携を要請した情報セキュリティ関係機関との間で情報共有を行う。

(3) 別紙

発生した事象に関し、報道発表・ウェブサイトでの発表等を行っている場合には、当該資料を別紙として添付することが望まれます。

また、発生した事象に係る検体等（届いた電子メール、添付されていたファイル、ログ等）は攻撃者に係る情報、対策の検討等に有益なものです。そのため、可能な限り情報連絡とともにＮＩＳＣに送付することが望まれます。検体等については、誤操作等による二次被害の防止とともに、セキュリティソフトによる駆除の防止を図るため、パスワードを設定したzip形式ファイルとするなど、安全な状態で取り扱う必要があります。具体的な送付方法等については継続して検討していくこととし、当面は都度問い合わせいただき対応することとします。

２．４　情報連絡の取扱いについて

(1) 秘匿性の確保

情報連絡は機微情報を含むことから秘匿性を確保するものとします。ＮＩＳＣは、付番、公開範囲等に基づき体系的に管理し、保存し、必要な時にいつでも参照できるようにします。

(2) 検体等

ＮＩＳＣが検体等を受領した際には、ＮＩＳＣにおいて分析を行うほか、あらかじめ連携を要請した情報セキュリティ関係機関と共有し、分析等を依頼することもあります。

３．ＮＩＳＣからの情報提供

３．１　情報提供の流れ

ＮＩＳＣは、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、情報セキュリティ関係機関、サイバー空間関連事業者及び重要インフラ事業者から提供される幅広いシステムの不具合等に関する情報を集約、分析等した上で、以下のいずれかのケースに該当する場合に情報提供を行います。

①セキュリティホールやプログラム・バグ等に関する情報を入手した場合等であって、他の重要インフラ事業者等においてもその情報に関係する重大な問題を生じるおそれがあると認められる場合。

②サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると

認められる場合。

③そのほか重要インフラ事業者等の情報セキュリティ対策に有効と考えられる場合。

ＮＩＳＣは、情報の提供元が特定されないよう、情報を加工するなど、不利益を被らないための適切な措置を講じた上で情報提供を行います。

また、ＮＩＳＣから重要インフラ事業者等への情報提供の範囲は、情報の提供元があらかじめ示す情報共有可能な範囲のうち、ＮＩＳＣが当該情報に関係すると考える重要インフラ分野とします。なお、情報の提供元が示す情報共有可能な範囲を越えて情報共有する必要があるとＮＩＳＣが認める場合には、その共有範囲の変更について情報の提供元との間で調整を行います。

ＮＩＳＣから重要インフラ事業者等への情報提供は、重要インフラ所管省庁へ行い、情報提供を受領した重要インフラ所管省庁がセプター事務局、あるいは、必要に応じて直接重要インフラ事業者等に展開することにより実施します。

情報提供の流れを図 6 に示します。

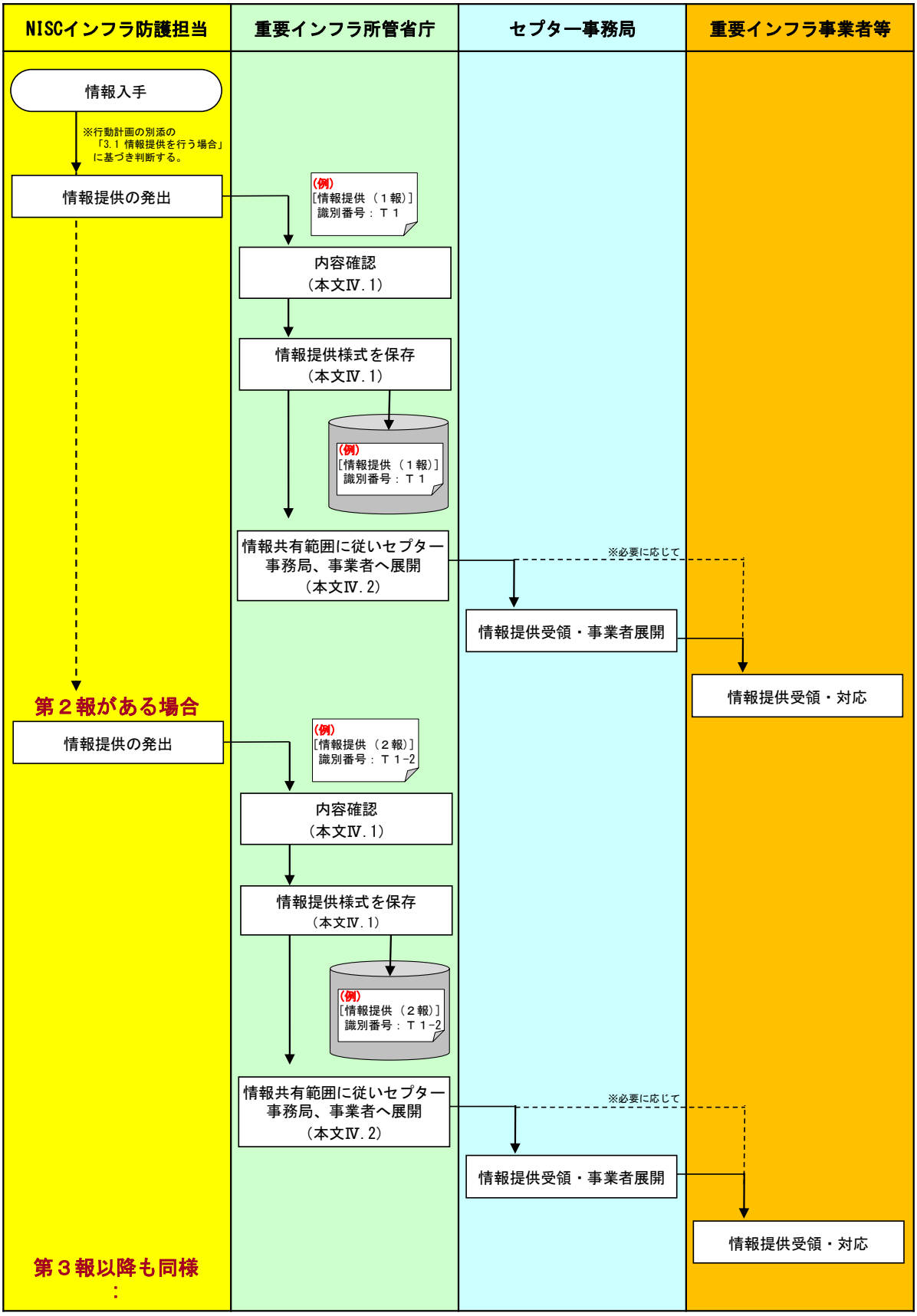

NISCインフラ防護担当
重要インフラ所管省庁
セプター事務局
重要インフラ事業者等
情報入手
※行動計画の別添の
「3.1 情報提供を行う場合」
に基づき判断する。
情報提供の発出
(例)
[情報提供（１報)]
識別番号：Ｔ１
内容確認
（本文Ⅳ.1）
情報提供様式を保存
（本文Ⅳ.1）
(例)
[情報提供（１報)]
識別番号：Ｔ１
情報共有範囲に従いセプター
事務局、事業者へ展開
（本文Ⅳ.2）
※必要に応じて
情報提供受領・事業者展開
情報提供受領・対応
第２報がある場合
情報提供の発出
(例)
[情報提供（２報)]
識別番号：Ｔ１-2
内容確認
（本文Ⅳ.1）
情報提供様式を保存
（本文Ⅳ.1）
(例)
[情報提供（２報)]
識別番号：Ｔ１-2
情報共有範囲に従いセプター
事務局、事業者へ展開
（本文Ⅳ.2）
※必要に応じて
情報提供受領・事業者展開
情報提供受領・対応
第３報以降も同様
：

図 6　情報提供の流れ

３．２　情報提供様式

情報提供様式及びその記載例をそれぞれ図 7 及び図 8 に示します。

ＮＩＳＣは、本様式に必要事項を記入し重要インフラ所管省庁に対し情報提供を行います。補足すべき事項等がある場合には別紙にてその内容の説明を行います。

なお、情報提供におけるＮＩＳＣへの問合せは、情報共有範囲内の重要インフラ所管省庁に限ります。

□警報　□注意喚起　□参考情報

（内閣官房→重要インフラ所管省庁）

情報提供様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号*

情報提供日時* 平成　　年　　月　　日

情報提供先* （所管省庁名及び分野名）	
情報共有範囲*	□Red = 宛先限り （情報提供先の重要インフラ所管省庁限り） □Amber=特定分野・関係者限り （情報提供先の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り） □Green=重要インフラ関係主体限り （重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り） □White=公開情報
	特記事項：

◆情報提供の内容　（別紙有無*：□有　□無 ）

項　目		情報の内容
脅威等の内容	①概　要	
	②対　象	
③対処方針		
④その他		

本件問合せ先（情報共有範囲からの問合せに限る。）
内閣サイバーセキュリティセンター
重要インフラ防護担当：
電話番号 ：
FAX番号 ：
電子メールアドレス ：

図 7　情報提供様式

□警報　□注意喚起　■参考情報

記載例　：青字

（内閣官房→重要インフラ所管省庁）

情報提供様式

（第　1　報*）

（*が付与された項目は必須事項）

識別番号*	Txxxxxx
情報提供日時*	平成 30 年 XX 月 XX 日 13:00

情報提供先* （所管省庁名及び分野名）	XX省（ZZ分野）、YY省（ZZ分野）、…
情報共有範囲*	□Red = 宛先限り （情報提供先の重要インフラ所管省庁限り） □Amber=特定分野・関係者限り （情報提供先の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り） ■Green=重要インフラ関係主体限り （重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り） □White=公開情報
	特記事項： 特になし

◆情報提供の内容　（別紙有無*：□有　■無）

項　目		情報の内容
脅威等の内容	①概　要	大手サイトfunifuniにおいてサイト改ざんが行われ、当該サイトへのアクセスに伴いマルウェア（悪意のあるソフトウェア）感染のおそれがあります。
	②対　象	XX年XX月XX日以降に http://example.co.jp/top(.)html にアクセスした場合。
③対処方針		○Webアクセスログ等の確認を行う。 ○マルウェアの通信先である次のIP及びドメインをブロックする。 XX.XX.XX.XX、ZZ.ZZ.ZZ.ZZ、example.com
④その他		特になし

本件問合せ先（情報共有範囲からの問合せに限る。）
内閣サイバーセキュリティセンター
重要インフラ防護担当：提供　花子
電話番号：　03-xxxx-xxxx
FAX番号：　03-xxxx-xxxx
電子メールアドレス：　teikyo.hanako@xx.go.jp

図 8　情報提供様式記載例

Ⅲ. 他の情報共有体制との関係

行動計画に基づく情報共有以外にも情報共有体制が構築されており、それらの情報共有体制との関係を以下に示します。

１. サイバーセキュリティ対処調整センター

サイバーセキュリティ対処調整センター（以下、「CS 対処調整センター」という。）は、2020 年東京オリンピック・パラリンピック競技大会（以下「2020 年東京大会」という。）に係るサイバーセキュリティ上の脅威・事案情報の収集・提供及びインシデント発生時の対処支援調整を行う中核組織であり、平成３１年４月１日に内閣官房に設置されており、ＮＩＳＣが中心となって運用を行っています。

2020 年東京大会に関するサイバー事案の関連情報共有と対処支援調整は、全体としては CS 対処調整センターが担当します。とりわけ、2020 年東京大会の安全・円滑な準備及び運営並びに持続性の確保のため、大会を支える重要なサービスを提供する事業者である「重要サービス事業者等」に対して、大会のサイバーセキュリティに係る脅威・インシデント情報を共有するとともに、必要があるときにはインシデント対処に対する支援調整を行います。

行動計画に基づく情報共有（①）と CS 対処調整センターを中心とした情報共有（②）との関係を図示すると図 9 のとおりです。重要サービス事業者等である重要インフラ事業者等は、①②それぞれに情報連絡を行うことも可能ですが、事業者側における業務負担の軽減を図る観点から、いずれか一方のみへの連絡も可能です。

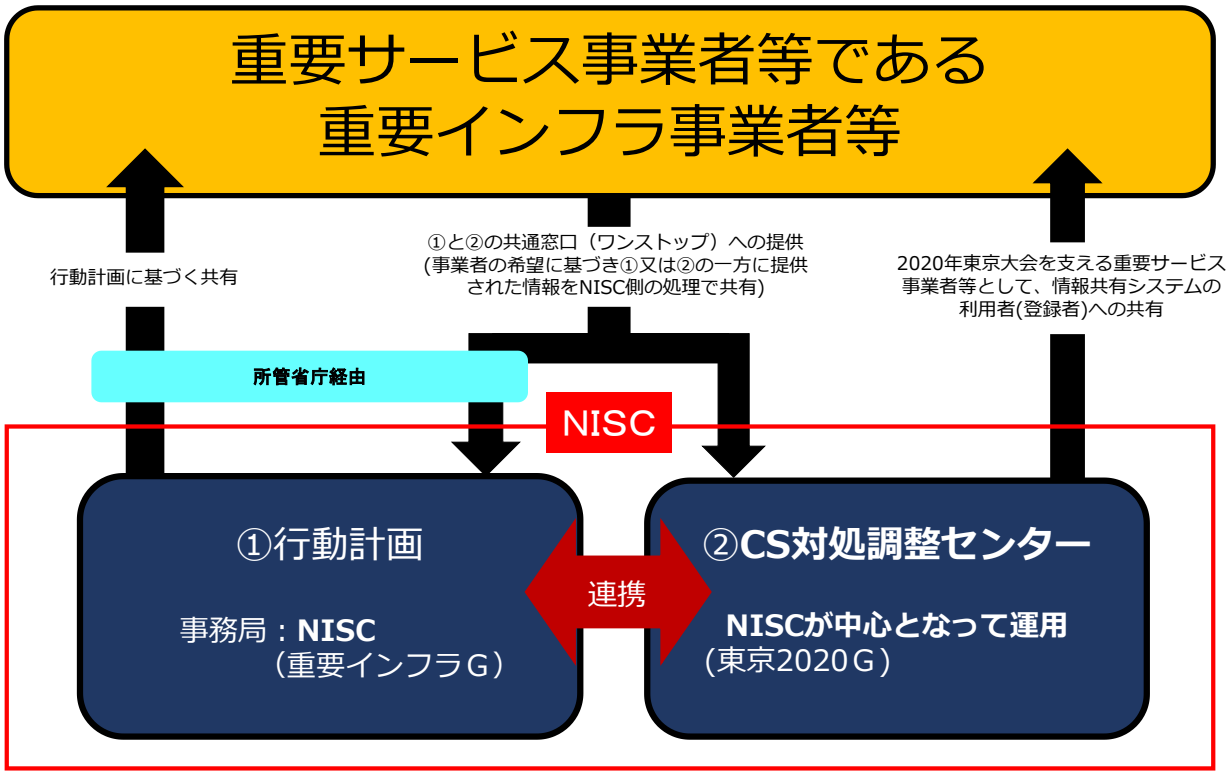


図 9　サイバーセキュリティ対処調整センターとの関係

２．サイバーセキュリティ協議会

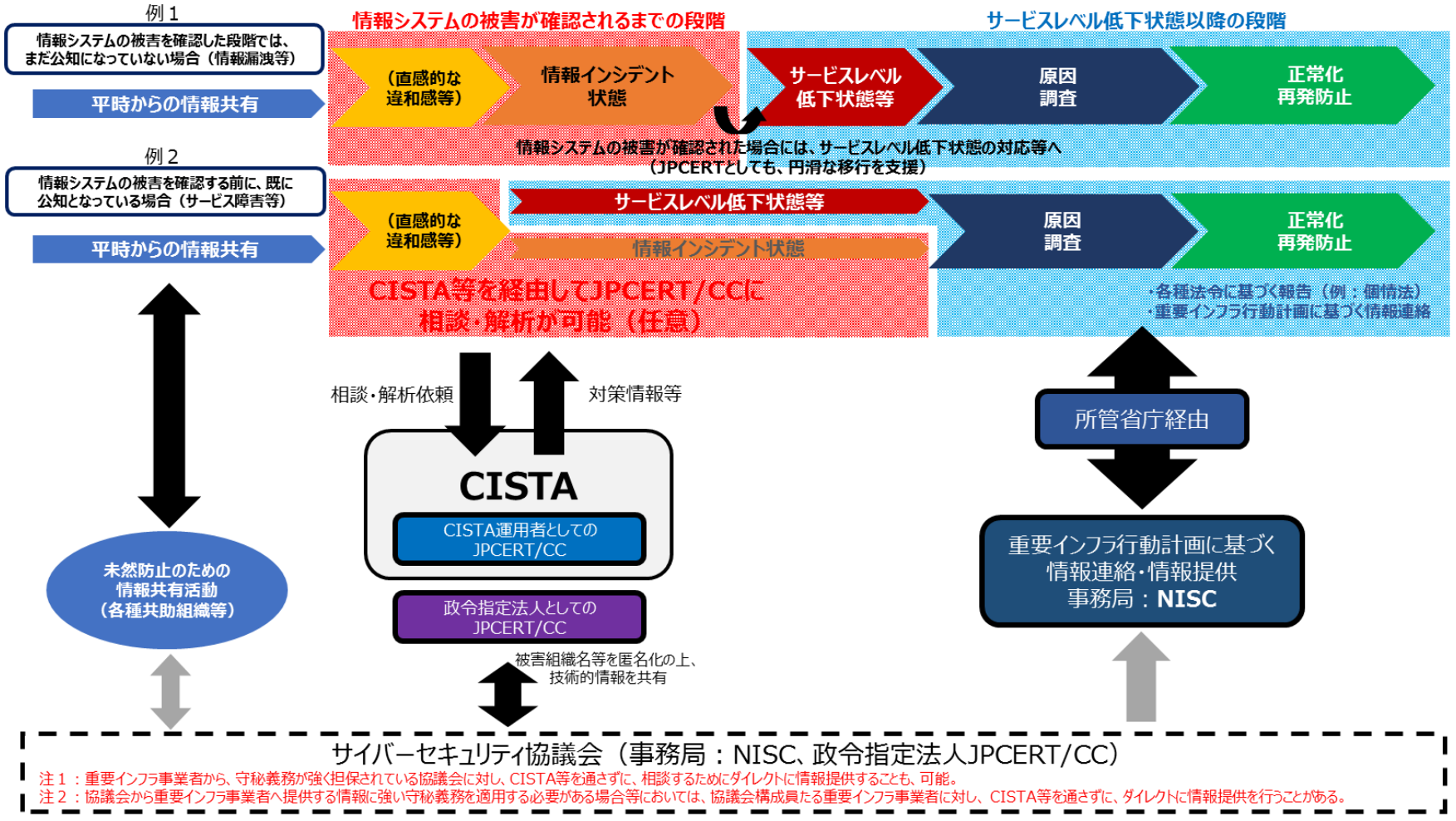
サイバーセキュリティ協議会は、サイバーセキュリティ基本法の規定に基づき平成３１年４月１日に創設された枠組みです。官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うものであり、主として、脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行うものです。協議会に加入し構成員となることにより対策情報等の受領ができるほか、情報インシデント状態の際に相談・解析依頼等を行うことができます。本枠組みにおいては法令で守秘義務を規定していることから、これまで外部に提供することがためらわれた情報の共有を図りやすいという利点があります。

本枠組みと行動計画に基づく情報共有との関係を図示すると図 10 のとおりです。

即ち、通常業務を行う中で「いつもと何か違う」といった直感的な違和感が生じた段階やサイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態（情報インシデント状態）といった、情報システムの被害が確認されていない早期の段階では、罰則により担保された守秘義務の下、安心して協議会に対し相談等を行うことが考えられます。その後、情報システムの被害が確認され、平常時（情報システムによるサービスが安全かつ持続的に

提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティエンジェンシープラン等に基づく対応を行っている状態（サービスレベルが低下状態）へ移行（※）した場合には、行動計画に基づく情報共有体制を活用することになります。

（※）なお、情報システムの被害を確認する前の段階で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まります。



※「情報インシデント状態」：ここでは、サイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態をいう。
※「サービスレベル低下状態」：ここでは、平常時（情報システムによるサービスが安全かつ持続的に提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティンジェンシープラン等に基づく対応を行っている状態をいう。なお、情報システムの被害を確認する前の段階（そもそも攻撃の存在を検知・認知していないケースを含む。）で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合（上記「例２」）においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まることとなる。
※「CISTA」：経済産業省予算事業「CISTA・検体分析機能の実用性調査及び開発」事業で運用する、情報共有・検体解析ポータルシステムをいう。
※「行動計画に基づく情報連絡」：ここでは、重フラ行動計画「2.1 情報連絡を行う場合」の対象となる情報のうち、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うことができる情報共有体制における取扱いが適すると考えられる情報（例：事業者等が検知した情報で非公知のもの、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をいう。）を除いたものの情報連絡をいう。
※協議会が重要インフラ以外の主体から得られた情報等に基づき重要インフラ分野においても早期対処が必要と判断した場合には、提供者の同意を得た上で行動計画側等に提供することがあり得る。これに対し、行動計画側等から協議会側に早期対処の情報連絡を行う必要が生じるケースは、現実的にほぼ想定されない。

図 10　協議会との関係

３．ＣＩＳＴＡ（Collective Intelligence Station for Trusted Advocates）

ＣＩＳＴＡは、一般社団法人 JPCERT コーディネーションセンター（以下、「JPCERT/CC」という。）と早期警戒情報受信組織との間で、脅威情報や分析結果及びそれらに対するフィードバック情報等の共有を行うシステムであり、JPCERT/CC が受信組織に対して脅威情報や分析結果、技術レポート等を提供し、受信組織が JPCERT/CC に対してフィードバックや検体等の提供を行うことにより、脅威情報を共有し、インシデントの未然防止や被害拡大の抑止を図るとともに、情報インフラ全体のリスク低減を目的としたものです。

４．サイバー情報共有イニシアティブ「Ｊ－ＣＳＩＰ」

Ｊ－ＣＳＩＰ（Initiative for Cyber Security Information sharing Partnership of Japan）は、独立行政法人情報処理推進機構（以下、「ＩＰＡ」という。）が情報の中継点・相談役として、国内の重要産業等に対するサイバー攻撃への対策を、各業界での自主的・互助的に行う情報共有活動です。ＩＰＡは、提供・共有された情報が重要な攻撃情報と判断した場合には、情報提供元組織に対して、所管省庁等への報告を勧めることがあります。また、この際ＩＰＡの見解やアドバイスが求められた場合は、相談対応の一環として可能な範囲で対応します。

Ⅳ. インシデント対応に資する情報等について

１．通常時から逐次確認すべき情報

１．１　ソフトウェア会社からの定例的なアップデート情報

(1) マイクロソフト株式会社

https://blogs.technet.microsoft.com/jpsecurity/2018/10/24/securityupdatereleaseschedule2019/

https://www.microsoft.com/ja-jp/safety/terms/securityupdates_whatis.aspx

セキュリティ更新プログラムは、ソフトウェアの脆弱性を修正するセキュリティ更新プログラムは、通常、米国日付の毎月第２火曜日に公開される。日本では、時差の関係上、毎月第２火曜日の翌日（第２水曜又は第３水曜）の公開となる。

ただし、脆弱性の危険性が高いと判断した場合は例外措置をとり、セキュリティ更新プログラムは可能な限り迅速に公開される。

(2)アドビシステムズ株式会社（Adobe Acrobat Reader）

https://helpx.adobe.com/jp/acrobat/release-note/release-notes-acrobat-reader.html

以下のセキュリティアップデートが公開される。リリースの時期については明言されていない。

・Continuous リリース（C）：新機能と機能拡張のほか、新しいセキュリティアップデート、既存機能のバグの修正、以前にリリースされた不定期のパッチの更新を含む機能リリース。

・四半期ごとのアップデート（Q）：機能の向上、新しいセキュリティアップデート、以前にリリースされた不定期のパッチ更新を含む定期的なアップデートです。Reader では、このようなアップデートが完全なインストーラーとして提供される場合があります。

・不定期のパッチ（OOC）：セキュリティの問題の修正を目的としたアップデート。

１．２　情報セキュリティ関係機関からの情報

(1) JPCERT/CC

https://www.jpcert.or.jp/at/

注意喚起として、深刻かつ影響範囲の広い脆弱性などの情報が告知される。情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内 CSIRT 業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等を

対象にしている。

(2) IPA

https://www.ipa.go.jp/security/index.html

重要なセキュリティ情報が、HP上で公開される。

重要なセキュリティ情報とは、放っておくと不正アクセスやデータが盗まれるなどの危険性が高いセキュリティ上の問題と対策について伝えるもので、インターネットを使っている多くの利用者が影響を受けるセキュリティ対策情報を対象にしている。

このほか、ＨＰで脆弱性対策情報（JVN）、他組織からの情報が掲載されている。

２．ＣＳＩＲＴ構築に資する情報

２．１　CSIRTマテリアル（JPCERT/CC）

https://www.jpcert.or.jp/csirt_material/

２．２　CSIRT構築に役立つ参考ドキュメント類（日本シーサート協議会）

https://www.nca.gr.jp/activity/build-wg-document.html

Ⅴ．関係法令等

１．関係法令

〇サイバーセキュリティ基本法（平成２６年法律第１０４号）

（定義）

第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（基本理念）

第三条　サイバーセキュリティに関する施策の推進は、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及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（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に関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

２～６　（略）

（重要社会基盤事業者の責務）

第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

〇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年サイバーセキュリティ戦略本部決定）

Ⅱ．本行動計画の要点（抄）

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。

②基本的な考え方

重要インフラ事業者等における情報セキュリティ対策は、一義的には当該重要インフラ事業者等が自らの責任において実施するものである。ただし、重要インフラ全体の機能保証の観点からは、各関係主体が連携して重要インフラ防護の目的を果たすために努力を払うことが必要である。このため、重要インフラ防護における関係主体が一丸となった取組を通じて、重要インフラ防護の目的を果たすとともに、あわせて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

・重要インフラ事業者等は、事業主体として、また社会的責任を負う立場として、それぞれに対策を講じ、また継続的な改善に取り組む。
・政府機関は、重要インフラ事業者等の情報セキュリティ対策に対して必要な支援を行う。
・取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

③　（略）

④重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実践すること。

・情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
・自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
・情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
・上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

Ⅲ. 計画期間内に取り組む情報セキュリティ対策（抄）

2.　情報共有体制の強化

2.3 重要インフラ事業者等の活動の更なる活性化

重要インフラ事業者等の活動を更に活性化するに当たり、重要インフラ事業者等の自らの活動に加え、セプター内、セプター間における情報共有の充実が期待される。

具体的には、重要インフラ事業者等においては、自ら積極的に情報共有に取り組むとともに、CSIRT 等の重要インフラサービス障害対応体制を構築・強化することが期待される。

２．用語の定義

安全基準等	関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称。ただし、指針は含まない。
関係主体	内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター、セプターカウンシル、情報セキュリティ関係機関及びサイバー空間関連事業者。
サービス維持レベル	機能保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。
サイバー空間関連事業者	重要インフラサービスを提供するために必要な情報システムに関係する、設計・構築・運用・保守等を行うシステムベンダー、ウィルス対策ソフトウェア等の情報セキュリティ対策を提供するセキュリティベンダー及びハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
システムの不具合	重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。
重要インフラ	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社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ分野として指定する分野。
重要インフラサービス	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。
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。
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省、国土交通省。
重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
情報共有	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）や情報セキュリティの確保に資する情報について、関係主体間

	で相互に提供し、共有すること。情報連絡及び情報提供の双方を含む。
情報システム	事務処理等を行うシステム、フィールド機器や監視・制御システム等の制御系のシステム等のＩＴを用いたシステム全般。
情報提供	情報セキュリティ対策に資するための情報を、内閣官房から重要インフラ事業者等へ提供すること等。
情報連絡	重要インフラ事業者等における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）を、重要インフラ事業者等から内閣官房に連絡すること等。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称（CEPTOAR）。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
防災関係府省庁	災害対策基本法（昭和36年法律第223号）第２条第３号に基づく指定行政機関等の、災害時の情報収集に関係する府省庁。
予兆・ヒヤリハット	システムの不具合が生じておらず、又は生じなかったものの、システムの不具合につながるおそれがあり、又はそのおそれがあった事象。